00862.023270 PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)	Examiner: Unassigned
Junichi HAYASHI	)	Group Art Unit: Unassigned
Application No.: 10/686,579	)	
Filed: October 17, 2003	)	
For: INFORMATION PROCESSING METHOD AND APPARATUS, COMPUTER PROGRAM, AND COMPUTER-READABLE STORAGE MEDIUM	)	December 4, 2003

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SUBMISSION OF PRIORITY DOCUMENT

Sir:

In support of Applicant's claim for priority under 35 U.S.C. § 119, enclosed is a certified copy of the following Japanese application:

JP 2002-304498, filed October 18, 2002.

Applicants' undersigned attorney may be reached in our Washington, D.C. office by telephone at (202) 530-1010. All correspondence should continue to be directed to our address given below.

Respectfully submitted,

Attorney for Applicant
Brian L. Klock
Registration No. 36,570

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200

BLK/lmj

10/686,579
Junichi HAYASHI
INFORMATION PROCESSING METHOD AND APPARATUS, COMPUTER PROGRAM, AND COMPUTER-READABLE STORAGE MEDIUM

CFM03270
US

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

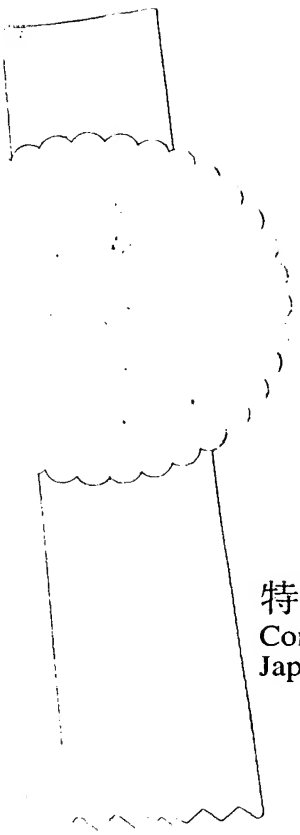
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年１０月１８日

出願番号
Application Number: 特願２００２－３０４４９８

[ST. 10/C]: [ＪＰ２００２－３０４４９８]

出願人
Applicant(s): キヤノン株式会社



２００３年１１月 ４日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号 出証特２００３－３０９０９７６

【書類名】　特許願
【整理番号】　4822046
【提出日】　平成14年10月18日
【あて先】　特許庁長官殿
【国際特許分類】　G06F　7/00
【発明の名称】　情報処理方法
【請求項の数】　1
【発明者】
【住所又は居所】　東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内
【氏名】　林　淳一
【特許出願人】
【識別番号】　000001007
【氏名又は名称】　キヤノン株式会社
【代理人】
【識別番号】　100076428
【弁理士】
【氏名又は名称】　大塚　康徳
【選任した代理人】
【識別番号】　100112508
【弁理士】
【氏名又は名称】　高柳　司郎
【選任した代理人】
【識別番号】　100115071
【弁理士】
【氏名又は名称】　大塚　康弘

【選任した代理人】

【識別番号】　100116894

【弁理士】

【氏名又は名称】　木村　秀二

【手数料の表示】

【予納台帳番号】　003458

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0102485

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報処理方法

【特許請求の範囲】

【請求項１】　タイル単位に圧縮符号化された画像データを入力し、暗号化する情報処理方法であって、

隣接する複数のタイルで１つのタイルグループを構成し、更に、隣接するタイルグループで１つの更なるタイルグループを構成することを繰り返すことで、タイルグループの階層構造を定義し、

符号化データで表現される画像全体から、最上位階層の暗号化鍵情報を生成し、

前記階層構造中の、上位に位置するタイルグループに対して生成された暗号化鍵情報に基づき、下位層に位置するタイルグループ或いはタイルに対する暗号化鍵情報を生成することを、末端に位置するタイルまで行ない、

前記タイルグループのツリー構造中の、所望とする階層の所望とするタイルグループを暗号化対象とする指定入力が与えられた場合、当該指定入力されたタイルグループに属する下位層の末端に位置するタイルに対して暗号化を行うよう設定し、

暗号化を行うよう設定された個々のタイルに対し、当該タイルに対して生成された暗号化キーを用いて暗号化処理を行ない、当該暗号化した符号化データ及び暗号化されていないタイルの符号化データを出力する

ことを特徴とする情報処理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、デジタル画像データの圧縮符号化したデータを暗号化する技術に関するものである。

【０００２】

【従来の技術】

従来、画像データなどを秘匿して伝送するために、画像データ全体の暗号化や

スクランブルなどが行なわれてきた。これは、予め画像データ全体を一つの暗号鍵を用いて暗号化し、この暗号鍵に対応する復号鍵を有するものだけが正しく復号することが可能であるようにする技術である。

【０００３】

しかし、階層構造を有する画像データの場合、その階層構造に応じて画像データの再生の可・不可を制御する目的で、画像全体ではなく階層構造毎に異なる暗号鍵を用いて暗号化処理が行うことが望まれる。また、画像データが複数のタイルから構成され、タイル毎に再生を制御する目的で、タイル毎に異なる暗号鍵を用いて暗号化処理が行われることが望まれる。更に、これらを合わせた場合として、複数のタイルから構成され、更に夫々のタイルが階層構造を有する画像データの場合、タイルと階層構造に応じた画像データの再生を制御する目的で、タイル中の階層構造毎に異なる暗号鍵を用いて暗号化処理が行われる。

【０００４】

このように、タイル及び階層構造毎に異なる暗号鍵を用いて暗号化することによりタイル、及び階層構造毎に画像データの再生を制御することが可能である。

【０００５】

【発明が解決しようとする課題】

しかしながら、暗号化された画像データの所定のタイル、及び階層構造を復号処理するためには、暗号化処理に用いた暗号鍵をすべて管理し、復号処理の際に適当な復号鍵を供給する必要がある。

【０００６】

また、このようにタイル、及び階層構造毎に異なる暗号鍵を用いて暗号化した場合、暗号化されるタイル及び階層構造と、それを復号するための復号鍵との対応付けをする必要があり、その鍵情報の管理が複雑化することは避けられない。

【０００７】

また、当然のことながら、その鍵情報が正しく管理されていない場合には、正しく復号処理を行うこともできない。

【０００８】

本発明は上記従来例に鑑みてなされたものであり、複数のタイル及び階層構造

を有する画像データに対して、タイル及び階層構造毎に異なる暗号鍵を用いて暗号化した場合にも、複数の鍵を管理する必要がない技術を提供することを目的とする。

【０００９】

【課題を解決するための手段】

この課題を解決するため、例えば本発明の情報処理方法は以下のような工程を備える。すなわち。

【００１０】

タイル単位に圧縮符号化された画像データを入力し、暗号化する情報処理方法であって、

隣接する複数のタイルで１つのタイルグループを構成し、更に、隣接するタイルグループで１つの更なるタイルグループを構成することを繰り返すことで、タイルグループの階層構造を定義し、

符号化データで表現される画像全体から、最上位階層の暗号化鍵情報を生成し、

前記階層構造中の、上位に位置するタイルグループに対して生成された暗号化鍵情報に基づき、下位層に位置するタイルグループ或いはタイルに対する暗号化鍵情報を生成することを、末端に位置するタイルまで行ない、

前記タイルグループのツリー構造中の、所望とする階層の所望とするタイルグループを暗号化対象とする指定入力が与えられた場合、当該指定入力されたタイルグループに属する下位層の末端に位置するタイルに対して暗号化を行うよう設定し、

暗号化を行うよう設定された個々のタイルに対し、当該タイルに対して生成された暗号化キーを用いて暗号化処理を行ない、当該暗号化した符号化データ及び暗号化されていないタイルの符号化データを出力する

ことを特徴とする。

【００１１】

【発明の実施の形態】

以下、添付図面に従って本発明に係る実施形態を説明する。

【００１２】

＜第１の実施形態＞

以下、図１４を用いて本実施の形態に適用されるシステム全体について説明する。

【００１３】

図１４に示すように、本実施の形態におけるシステムは、暗号化処理部（或いは暗号化する装置）１４１、アクセス鍵生成部（或いはアクセス鍵生成装置）１４２、及び復号処理部（或いは復号装置）１４３から構成される。

【００１４】

暗号化処理部には、コードストリームｃ（画像データの符号化データであるが、その詳細は後述）が入力され、コードストリームｃからコンテンツ鍵ｃｋ、及び暗号化されたコードストリームｃ’が出力される。アクセス鍵生成処理部１４２は、このコンテンツ鍵ｃｋ、及びアクセスレベルａｎを入力し、アクセス鍵ａｋを生成する。そして、復号処理部１４３は、アクセス鍵ａｋ、及び暗号化されたコードストリームｃ’が入力され、復号処理されたコードストリームｃ’’が出力される。ここで、ｃ’＝ｃ’’である場合、暗号化する以前の画像データに復元されることになる。

【００１５】

本実施形態においては、アクセス鍵生成部１４２、及び復号処理部１４３は互いに耐タンパー（耐改ざん）であるようにする。例えば、暗号化処理部１４２はデジタルカメラで撮影した画像を暗号化し、インターネット上のＷｅｂサーバやＦＴＰサーバにアップロードする装置で実行され、アクセス鍵生成処理部１４２はアクセス鍵を発行するサーバで実行され、復号処理部１４３は暗号化された画像データをダウンロードするネットワーククライアントで実行されるようにする。

【００１６】

［暗号化処理部］

以下、図１を用いて本実施形態に適用される暗号化処理部（機能）を説明する。

【００１７】

図１に示すように、本実施形態における暗号化処理部は、コードストリームｃを入力し、入力されたコードストリームからコードストリーム鍵ｃｋ、及びコードストリームｃが暗号化された暗号化コードストリームｃ’が生成され、生成されたコードストリーム鍵ｃｋ、及び暗号化コードストリームｃ’が出力される。

【００１８】

本実施形態における暗号化処理部は、暗号化タイルパート指定部１１、鍵行列生成部１２、暗号化部１３から構成される。

【００１９】

なお、ここで説明する暗号化処理はソフトウェア処理により実現されても良い。その場合には、上記各部は上記処理に必要な機能を概念的なものとして捉えたものと考慮されるべきものである。

【００２０】

まずはじめに、暗号化タイルパート指定部１１の処理の詳細を説明する。暗号化タイルパート指定部１１には、コードストリームｃが入力され、入力されたコードストリームから、タイルパートを抽出され、抽出されたタイルパートのうち暗号化対象とするタイルパートを指定するための暗号化タイルパート情報ｔａを出力する。

【００２１】

そこで先ず、本実施形態におけるコードストリーム、及びタイルパートについて説明する。コードストリームとは、画像データを圧縮符号化した際の符号列である。本実施形態においては、ＩＳＯ／ＩＥＣ ＪＴＣ１／ＳＣ２９／ＷＧ１ １０９１８－１において標準化されている、通称ＪＰＥＧ２０００と呼ばれる圧縮符号化方式によって符号化された符号列のことをコードストリームと呼ぶ。

【００２２】

ＪＰＥＧ２０００の圧縮符号化時において、画像は先ず複数の矩形領域に分割され、矩形領域毎にウェーブレット変換により独立に符号化処理が施される。この矩形領域を「タイル」と呼ぶ。更に、符号化されたタイルに対応するコードストリームは、少なくとも一つ以上のタイルパートと呼ばれる領域に分割できる。

【００２３】

より詳しく説明すると、１つのタイルに対し１回目のウェーブレット変換により得られる成分係数は公知の通り、ＬＬ１、ＬＨ１、ＨＬ１、ＨＨ１の各周波数成分領域を生成する。このうち、｛ＬＨ１＋ＨＬ１＋ＨＨ１｝を１つのパートとして扱う。２回めのウェーブレット変換はＬＬ１に対して行うが、このとき生成されるＬＬ２、ＬＨ２、ＨＬ２、ＨＨ２のうち｛ＬＨ２＋ＨＬ２＋ＨＨ２｝も１つのパートとして扱う。

【００２４】

また、更に、ＬＬ２に対して更なるウェーブレット変換（３回めのウェーブレット変換）を行う場合には、その結果生じる｛ＬＨ３＋ＨＬ３＋ＨＨ３｝がパートとして扱われ、残りのＬＬ３が単独のパートとして扱われる。この後、量子化、エントロピー符号化が施され符号化される。上記のタイルパートとは、上記のウェーブレット変換を行う毎に生成された周波数成分の集合の符号化結果を示している。以上が１つのタイルの符号が複数のタイルパートの符号で構成される理由である。

【００２５】

なお、ＪＰＥＧ２０００では、全タイルに対して固定回数のウェーブレット変換を行ういう決まりはない。換言すれば、タイル毎に、ウェーブレット変換の回数は異なっていてもよいことになっている。

【００２６】

以下の実施形態におけるタイルパートとは、上記のような意味を前提にして説明するが、これ以外については後述することとする。

【００２７】

タイル、及びタイルパートの具体例を図２を用いて説明する。図２（ａ）は、ある画像をタイルに分割した際の例である。図２（ａ）において、２１は画像全体を８×８＝６４個のタイルに分割した例を示している。また、図２（ｂ）は、ある１つのタイルを符号化した際のコードストリームの例を示している。図２（ｂ）に示す例では、１つのタイルは２２、２３、２４、２５の４つのタイルパートで構成されていることを示している。

【００２８】

ここで、タイルパートについて説明する。ＪＰＥＧ２０００において、タイルは複数のタイルパートとよばれるいくつかに分割することが可能である。タイルパートは、全てのタイルの中でのタイルパートの順序が保たれさえすれば、異なったタイルからのタイルパートを挟み込むことが可能である。例えば、

タイルインデックス０のタイルパートインデックス０

タイルインデックス１のタイルパートインデックス０

タイルインデックス０のタイルパートインデックス１

タイルインデックス１のタイルパートインデックス１

：

のようにコードストリームを構成することにより、複数のタイルに属するタイルパートを平行に再生することができる。

【００２９】

更に、夫々のタイルパートは、ヘッダ部分とデータ部分から構成されている。ここでヘッダ部分とは、データ部分の伸張復号のために必要な種々の情報を格納するための領域であり、タイルパートヘッダと呼ぶ。図２（ｂ）では、タイルパート２２が、ヘッダ部分２６、データ部分２７で構成されていることを示しているが、他のタイルパートも同様である。

【００３０】

また、ＪＰＥＧ２０００においては、コードストリームｃはコードストリームｃの復号量に応じて様々な再生方法を実現できるように、所望の再生方法に応じてデータを並べることができる。このようなデータの並べ方をプログレッションオーダと呼ぶ。例えば、復号量の少ない段階では低解像度の画像を再生し、復号量が多くなるにつれてより高解像度の画像を再生するようなプログレッションオーダや、復号量に応じて画質が向上するようなプログレッションオーダでコードストリームｃを構成できる。

【００３１】

本実施形態においては、コードストリームｃは、予め、所望のアクセス制御の方法や度合いに応じたプログレッションオーダ、及びタイルパートで圧縮符号化

されていることを前提とする。

【００３２】

これに関して、例を用いて説明する。例えば、所定のタイルを３レベルの解像度に応じたアクセス制御をしたい場合を想定する（１つのタイルが３つのタイルパートで構成される場合に相当するものであり、ウェーブレット変換を２回行う場合と考えると分かりやすい）。この場合には、予め、解像度を優先させたプログレッションオーダとなるようにタイルを圧縮符号化し、更にタイルを３つのタイルパートに分割しておく。

【００３３】

尚、本実施形態においては入力されるコードストリームｃが、予め、所望のアクセス制御の方法や度合いに応じたプログレッションオーダ、及びタイルパートを用いて圧縮符号化されていることを前提としているが、本発明はこれに限定されることはない。即ち、コードストリームｃが所望のアクセス制御の方法や度合いに応じたプログレッションオーダやタイルパートを用いて圧縮符号化が施されていない場合には、コードストリームｃが入力された後に、所望のアクセス制御の方法や度合いに応じたプログレッションオーダやタイルパートを用いて圧縮符号化し直すようにすれば良い。

【００３４】

次にタイルグループについて説明する。本実施形態においては、複数のタイルをグループ化して扱う。グループ化された１つのタイルのグループを「タイルグループ」と呼ぶ。本実施形態においては、グループ化の一例として隣接する２×２の４つのタイルを１つのタイルグループとして扱う。更に、２×２の４つのタイルグループを１つのタイルグループとする。こうして画像全体がひとつのタイルグループとなるまでグループ化を繰り返し行う。

【００３５】

タイルグループ化の具体例を図３を用いて説明する。図３の３１には、図２に示した例と同様に画像全体を６４個のタイルに分割した例を示す。３２には、３１において隣接する４個のタイルをグループ化し、画像全体を１６個のタイルグループで表現した例を示す。更に、３３には、３２において隣接する４個のタイ

ルグループをグループ化し、画像全体を４個のタイルグループで表現した例を示す。更に、３４には、３３において隣接する４個のタイルグループをグループ化し、画像全体を１個のタイルグループで表現した例を示す。

【００３６】

以上、説明したタイル、タイルパート、及びタイルグループの構成の具体例を図４Ａを用いて説明する。

【００３７】

図４Ａには、画像全体が６４個のタイルに分割された場合のタイルグループ、タイル及びタイルパートの構成の例を示す。図４Ａに示すように、本実施形態におけるタイルグループ、及びタイルパートは画像全体をルートノードとするツリー構造で表現できる。各ノードがタイルグループ、及びタイルパートに対応する。

【００３８】

図４Ａにおいてルートノードは画像全体（図３における３４）を示す。ルートノード（レベル０）は、レベル１に属する４つの子ノードに対応するタイルグループ（図３における３３）から構成されている。ここで、レベルとはツリー構造における各階層構造の段階を示すインデックスである。ルートノードをレベル０であると定義する。更に、ツリー構造における親子の関係を親から子に向かって１回たどる毎に、レベルを１つずつ増やすようにする。

【００３９】

すると、レベル１に属するノードは、夫々、レベル２に属する４つの子ノードに対応するタイルグループ（図３における３２）から構成されると言い換えることができる。同様に、レベル２に属する４つの子ノードは、夫々、レベル３に属する４つの子ノードに対応するタイル（図３における３１）から構成されることになる。そして、レベル４以降は、その直後のレベルに属するひとつの子ノードに対応するタイルパートからだけ構成されている。

【００４０】

更に、レベル４以降は、ツリー構造において、大きなタイルパートインデックスが親ノードに対応し、タイルパートが小さくなる順に、ツリー構造を形成して

いることに注意する（タイルパートのインデックスが０のタイルパートは、最も低周波成分領域に対応する）。

【００４１】

この様に、本実施形態におけるタイルグループ、及びタイルパートはツリー構造で表現できる。

【００４２】

更に、タイル、タイルパート、及びタイルグループは夫々を特定することが可能なインデックスが割り当てられる。

【００４３】

タイルには、“０”を起源として画像の左上に位置するタイルからラスタ順にタイルインデックスが割り当てられる。

【００４４】

また、タイルパートには、夫々のタイルにおいて“０”を起源としてコードストリームをデコードする順にタイルパートインデックスが割り当てられる。実施形態では、ＪＰＥＧ２０００を例にして説明しているので、タイルパートインデックス“０”は、最も低周波成分領域を指し示すものであり、以下、高周波成分になるにつれてタイルパートインデックスは大きくなる。

【００４５】

更に、タイルグループは、夫々を構成する下位レベルのタイルグループ若しくはタイルにおいて“０”を起源として画像の左上に位置するタイル、タイルグループからラスタ順にインデックスが割り当てられる。割り当てられたインデックスは、その親のインデックスに連結されて、タイルグループインデックスとして割り当てられる。要するに、復号する際に、必須のもの程、タイルパートインデックスの数字が小さいように割り当てる。

【００４６】

以降の説明においては、以上説明したようにタイルグループインデックスが割り当てられるようにするが、本発明はこれに限定されることなく、種々のタイルグループインデックスの割り当て方が可能である。例えば、各ノードの親のタイルグループインデックスに子ノードのグループインデックスを連結させて表現す

ることも可能である。子ノードは、親のタイルグループ内においてラスタ順に０からインデックスが割り当てられるようにする。

【００４７】

この割り当て方によれば、図４Ａにおける「１－０」で示されるタイルグループは、タイルインデックスで表現すると「０－０」と表現できる。同様に、「２－１」は、「０－０－１」と表現できる。

【００４８】

図４Ｂは、図４Ａと等価のツリー構造を、タイルインデックス＆タイルパートインデックスで示したものである。なお、図示において、例えば「０－０－０－０（３）」における「０－０－０－３」はタイルインデックスであることは上記の通りであるが、末尾の「（３）」はタイルパートインデックスである。タイルパートインデックスが小さいほど優先的に復号する、すなわち、低周波成分の符号化データであることを示している。

【００４９】

以上、本実施形態におけるコードストリーム、タイルグループ／タイル／タイルパートの構造、及びタイルグループインデックス／タイルインデックス／タイルパートインデックスについて説明した。

【００５０】

本実施形態における暗号化タイルパート指定部１１では、入力されたコードストリームｃ中のメインヘッダ部分、及びタイルパートヘッダ部分に属する情報を読み出し、タイル、タイルパート、及びタイルグループの構成を解析する。そして、暗号化の対象とするタイルグループ、タイル、及びタイルパートを指定し、暗号化タイルパート情報ｔａとして出力する。

【００５１】

暗号化の対象とするタイルグループ、タイル、及びタイルパートは、ユーザによって明示的に指定されても良いし、ＲＡＭやＨＤなどに予め記憶されている情報を用いるようにしても良い。

【００５２】

ユーザによって指定されるようにする場合、コードストリームｃを解析した結

果を、例えば図４Ｂに示すようなツリー構造として、モニタなどを用いてユーザに示すようにする。そして、ユーザは所望のタイルグループ、或いはタイルパートに対応するノードを指定する。或るタイルグループ或いはタイルパートが指定されると、その指定された位置から図示の破線で示される位置に向かう方向に存在するタイルグループ或いはタイルパートも暗号化する対象として決定される。

【００５３】

例えば、図４Ｂにおいて、「０－０－０－０（２）」が指定された場合、「０－０－０－０（２）」とその上位にある「０－０－０－０（３）」が暗号化対象として決定される。ただし、タイル「０－０－０－１（１）」乃至「０－０－０－３（０）」は暗号化対象とはならず、解読キーがなくても復号し再現できることを意味する

また、タイルグループ「０－０」が指定された場合には、破線に向かう方向、すなわち、その下位のタイルグループ「０－０－０」、「０－０－１」、「０－０－２」、「０－０－３」が暗号化対象として決定される。ここで、タイルグループ「０－０－０」について着目すると、そのタイルグループにはタイル「０－０－０－０」乃至「０－０－０－３」が含まれるので、それらも暗号化対象として決定され、結果的に、それぞれのタイルの全タイルパートも暗号化対象として決定されることになる。すなわち、１つのタイルグループを指定した場合、そのタイルグループに含まれる下位のタイルグループ、最終的には下位に位置する各タイルの全タイルパートが暗号化対象して決定されることになる。

【００５４】

このことは、例えば解像度に応じてアクセス制御をする場合、高解像度に対するアクセス権を有するユーザは、自動的に、低解像度に対するアクセス権を有することを意味する。また、タイルグループを指定した場合には、そのタイルグループに属するタイル、更にタイルパートは全て暗号化対象とすることを意味する。

【００５５】

以上、説明した様に暗号化対象となるタイル、或いはタイルパートが決定される。暗号化対象として指定されたタイルパートは暗号化対象タイルパート情報ｔ

ａとして出力される。ここで、ｔａはタイルインデックスと、そのタイルに属するタイルパートのうち暗号化されるタイルパートのインデックスの最小値との組で構成される。

【００５６】

図５に画像全体が６４個のタイルから構成されるコードストリームに対するｔａの一例を示す。図５に示すように、例えばタイルインデックス０のタイルは暗号化されるタイルパートの最小値が０となっており、これはこのタイルに属するタイルパートを全て暗号化することを意味する。一方、タイルインデックス１のタイルは暗号化されるタイルパートの最小値が２となっており、これはこのタイルに属するタイルパートのうちタイルパートインデックスが０、及び１のタイルパートは暗号化されず、タイルパートインデックスが２以上のタイルパートに対して暗号化することを意味する。

【００５７】

なお、ユーザが暗号化対象を決定する場合（ｔａを決定する場合）には、特定の暗号化させる１つのタイル、或いは、タイルパートを指定しても良いが、暗号鍵無しで再現できる最高解像度（或いは暗号化鍵で再現する最低解像度）の限界を指定することが望ましい。そこで、図４Ｂのような画面を表示させたとき、縦一列のタイルグループ或いはタイルパートを一度に設定できるようにするため、縦線を表示し、その表示位置をポインティングデバイスで水平に移動させることで、暗号化する対象を決定するようにすることが望ましいであろう。ただし、ここでは、個々にユーザが指定する場合を説明することとする。

【００５８】

以上、説明したように、暗号化タイルパート指定部１１から、暗号化対象タイルパート情報ｔａが出力され、暗号化部１３に入力される。

【００５９】

次に、鍵行列生成部１２の処理の詳細を説明する。鍵行列生成部１２には、コードストリームｃが入力され、入力されたコードストリームｃから、鍵行列ｋａが生成され、生成された鍵行列ｋａ及びコードストリーム鍵ｃｋが出力される。

【００６０】

ここで、鍵行列生成部１２で実行される鍵行列生成処理について図６を用いて、詳細に説明をする。図６は鍵行列生成部１２で実行される鍵行列生成処理を示すフローチャートである。

【００６１】

まず、ステップＳ６１でコードストリーム鍵ｃｋが生成される。コードストリーム鍵ｃｋは、コードストリームｃのハッシュ値として次式（式（１））の様に算出される。

ｃｋ＝Ｋ（０）＝Ｈ（ｃ）　　（式１）

ここで、Ｈ（）は、一方向性（不可逆）、及び衝突耐性を有する関数であり、例えば、ハッシュ関数や、ＤＥＳなどの暗号化処理などが適用可能である。コードストリーム鍵ｃｋとは、図４に示したツリー構造におけるルートノードに対応する値であり、入力した１画像分のデータに基づいて生成する。

【００６２】

次いで、ステップＳ６２において、パラメータｉを初期値“１”、そしてパラメータｊを“０”に初期化する。パラメータｉは前述したツリー構造におけるレベルを示すインデックスであり、パラメータｊは前述した各レベルにおけるノードを表すインデックスである。特に、ｉとｊの組み合わせ（ｉ，ｊ）をタイルグループインデックスと呼ぶ。

【００６３】

次のステップＳ６３では、タイルグループインデックス（ｉ，ｊ）のタイルグループ鍵が生成される。タイルグループ鍵は、その親のタイルグループ鍵、及びタイルグループインデックス（ｉ，ｊ）のハッシュ値として式（２）の様に算出される。

Ｋ（ｉ，ｊ）＝Ｈ（Ｋ（ｉ－１，ｋ），ｉ，ｊ）　　（式２）

ここで、ｋはタイルグループ（ｉ，ｊ）の親ノードに対応するノードを表すインデックスである。即ち、親ノードに対応するタイルグループ鍵Ｋ（ｉ－１，ｋ）と、生成するタイルグループ鍵に対応するノードのタイルグループインデックス（ｉ，ｊ）とからタイルグループ鍵が生成される。しかしながら、本発明はこれに限定されることなく、親ノードに対応する鍵と、生成するタイルグループ鍵

に対応するノードに含まれるタイルインデックスとからタイルグループ鍵を生成するようにしてもよい。例えば、生成するタイルグループに対応するノードから順に木（ツリー）をたどり、タイルに対応するノードを調べ、当該タイルのタイルインデックを用いるようにすれば良い。要するに、上位ノード（ルートノード側にあるノード）に対する鍵ｃｋと、その下位（下層）方向にあるノードのインデックスに基づいて、下位にあるノードの鍵を派生することを順に繰り返すことになる。

【００６４】

ステップＳ６４では、レベルｉにおいて全てのノードに対応するタイルグループ鍵が生成されたか否かが判定される。判定結果が真の場合はステップＳ６６に進み、判定結果が偽の場合はステップＳ６５に進む。

【００６５】

ステップＳ６５では、パラメータｊが１だけ増やされ、その後ステップＳ６３が再度処理される。つまり、パラメータｉで示されるレベルに属する全タイルグループについて鍵が生成されることになる。

【００６６】

一方、パラメータｉで示されるレベルに対するタイルグループ鍵が生成されると、処理はステップＳ６６に進み、変数ｊを初期化し、全てのレベルが処理されたか否かが判定される。判定結果が真の場合はステップＳ６８に進み、判定結果が偽の場合はステップＳ６７に進んで、次のレベルの処理を行うべく、パラメータｉを１だけ増加させ、ステップＳ６３以降の処理を繰り返す。

【００６７】

さて、処理がステップＳ６８に進むとき、末端のノード、すなわち、タイルグループではなく、個々のタイルに対する鍵の生成が行われると、処理はステップＳ６８に進む。

【００６８】

ステップＳ６８では、パラメータｍを“０”、パラメータｎを“Ｎ－１”で初期化する。ここで、パラメータＮとは、タイルｍを構成するタイルパートの総数である。

【００６９】

ステップＳ６９では、タイルインデックスｍ、タイルパートインデックスｎに相当するタイルパート鍵が生成される。タイルパート鍵は、その親のタイルパート鍵のハッシュ値として式（３）の様に算出される。

Ｋ（ｍ，ｎ＋１）＝Ｈ（Ｋ（ｍ，　ｎ））　　（式３）

生成されたタイルパート鍵は鍵行列ｋａとして記録される。ここで、鍵行列ｋａの例を図７を用いて説明する。図７には本実施形態に適用可能な鍵行列ｋａの一例を示す。従って、或るタイルパートの最も大きなインデックスを持つタイルパートの鍵は、そのタイルパートが属するタイルに対して生成された鍵（ステップＳ６３で生成された鍵）を元に生成し、以下、タイルパートのインデックスが小さくものは、それより１つ大きなインデックスのタイルパートに与えられたキーを用いて派生することになる。

【００７０】

図７は、画像全体が６４個のタイルから構成され、タイルパートの数の最大が５である場合の鍵行列ｋａの例を示している。図７に示すように、鍵行列ｋａの各行はタイルに相当し、各列はタイルパートに相当する。行列の要素値としては、ステップＳ６８で算出したタイルパートの鍵を記録する。タイルパートが存在しない要素にはＮＵＬＬなど記録するようにする。

【００７１】

ステップＳ６９に続いてステップＳ７０が処理される。このステップＳ７０では、タイルパートインデックスｎに属する全てのノードに対応するタイルパート鍵が生成されたか否かが判定される。判定結果が真の場合はステップＳ７２に進み、判定結果が偽の場合はステップＳ７１に進んでパラメータｎを“１”だけ減じ、ステップＳ６９の処理を行うことになる。

【００７２】

こうして、タイルインデックスｍで示される全タイルパートに対する処理が終わると、ステップＳ７２に進み、変数ｎを初期化し、全てのタイルが処理されたか否かが判定される。判定結果が真の場合は、鍵行列生成処理を終了し、判定結果が偽の場合はステップＳ７３に進み、次のタイルに対する処理を行うべくパラ

メータｍを“１”け増加させ、ステップＳ６９以降の処理を繰り返すことになる。

【００７３】

以上、説明したように、鍵行列生成処理により鍵行列ｋａが生成される。生成された鍵行列ｋａは暗号化部１３に入力される。

【００７４】

次に、暗号化部１３の処理の詳細を説明する。暗号化部１３は、コードストリームｃ、暗号化対象タイルパート情報ｔａ、及び鍵行列ｋａを入力し、暗号化タイルパート情報ｔａに示されたコードストリームｃのタイルパートを、鍵行列ｋａに記録されているタイルパート鍵を用いて暗号化し、暗号化されたコードストリームｃ’を出力する。具体的には次の通りである。

【００７５】

暗号化部１３は、先ず、暗号化タイルパート指定部１１からの暗号化タイルパート情報ｔａに基づき、実際に暗号化対象となるタイルパートであるかどうかを判断するための暗号化タイルパート行列を生成する。暗号化タイルパート行列の例は図８に示す通りである。図示の行列において、行はタイルを表し、列はタイルパートを表す。更に、要素の値としては、暗号化対象とならないタイルパートは０、暗号化対象となるタイルパートは１、存在しないタイルパートは２で示されている。「２」が格納される理由は、タイルをウェーブレット変換する際の変換回数がタイル毎に異なる、すなわち、各タイルのタイルパートの個数が異なっていても構わないことに対処するためである。因に、図８の場合には、ウェーブレット変換の最大回数は５回であることを示している（ウェーブレット変換回数＋１がタイルパートの個数であることは既に説明した）。

【００７６】

暗号化タイルパート情報ｔａには、各タイル中で暗号化されるタイルパートインデックスの最小値が記録されており、更に本実施形態においては、夫々のタイル中で、暗号化タイルパート情報ｔａに記録されたタイルパートインデックスよりも大きな値を持つタイルパートは暗号化されるために、図５に示す暗号化タイルパート情報からは、図８に示すように暗号化対象となるタイルパートが特定さ

れる。

【００７７】

次に、暗号化対象タイルパート行列と鍵行列ｋａを比較し、暗号化対象タイルパート行列の要素値が１であるタイルパートに対して、鍵行列ｋａ中の同じ座標に位置する鍵を用いて、コードストリームｃ中のタイルパートを暗号化する（暗号化対象タイルパート行列の要素値が０のタイルパートについては暗号化しない）。こうして、暗号化対象となっているタイルパート全てに対して暗号化を施し、コードストリームｃ中の該当するタイルパートのデータは、暗号化されたタイルパートのデータで置換えられ、出力される。

【００７８】

また、暗号化したタイルパートは、該タイルパートが暗号化されていることを示すための情報Ｉｎｆをタイルパートヘッダに記録しておく。これは、後述する暗号復号処理の際に、タイルパートが暗号化されているか否かを判定するために用いる。

【００７９】

更に、ＪＰＥＧ２０００においては、タイルパートを構成するコードストリームｃは、パケットと呼ばれる単位から構成されている。そして、パケットはヘッダ部分とデータ部分から構成されている。本実施形態においては、ヘッダ部分は暗号化せずに、データ部分だけを暗号化するようにする。このように暗号化することによって、例え暗号化したとしても、画像として正しく伸張復号することが可能である。

【００８０】

暗号化の方法としては、本実施形態においては特に限定せず、ＤＥＳ（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）や、ＡＥＳ（Ａｄｖａｎｃｅｄ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）など種々の暗号アルゴリズムを適用可能である。

【００８１】

以上の様に、暗号化タイルパート行列に示された全てのタイルパートが暗号化されたコードストリームは、暗号化コードストリームｃ’として出力される。以

上、図１４における暗号化処理部１４１について説明した。

【００８２】

上記本実施形態における暗号化処理部１４１は、一般に、パーソナルコンピュータ等の情報処理装置で実現できることは容易に類推できよう。また、パーソナルコンピュータ等の情報処理装置で、上記機能を実現すれば良いわけであるから、実施形態での特徴は情報処理方法、更には、コンピュータプログラムや、コンピュータプログラムを格納するＣＤＲＯＭ等のコンピュータ可読記憶媒体にまで及ぶものである。

【００８３】

[アクセス鍵生成処理部]

次に、図９を用いて本実施形態に適用されるアクセス鍵生成部（機能）を説明する。

【００８４】

図９に示すように、アクセス鍵生成部は、コードストリーム鍵ｃｋ、及びアクセスを許可するインデックスａｎが入力され、入力されたコードストリーム鍵ｃｋからアクセスを許可するインデックスａｎに対応するアクセス鍵ａｋ（暗号化を解除する鍵）が生成され、生成されたアクセス鍵ａｋが出力される。ここで、アクセスを許可するインデックスａｎとは、アクセスを許可するタイルグループインデックス、或いはタイルとタイルパートインデックスである。

【００８５】

図４に示したように、本実施形態においては、タイルグループ、及びタイルパートはツリー構造で表現できる。図４に示したツリー構造を構成するノードのうち、ひとつのノードを、アクセスを許可するインデックスａｎで指定し、指定されたノードに対応するアクセス鍵を生成する。

【００８６】

指定されたノードのアクセス鍵を生成する方式としては、入力されたコードストリーム鍵ｃｋをルートノードに対応させ、図６に示したような方法で順に各ノードに対応する鍵を生成し、これをノードのインデックスがアクセスを許可するインデックスａｎになるまで繰り返すようにすれば良い。

【００８７】

生成されたアクセス鍵は、図１０に示すようなフォーマットに従ってａｋとして出力される。図１０に示すように、ａｋは、アクセス鍵、アクセス鍵が対応するタイルグループ或いはタイルパートのインデックス、及びタイルパートインデックスかタイルグループインデックスかを示す情報から構成される。図１０に示すようなフォーマットに格納された後、ａｋは後述する暗号復号処理部に渡される（実際は、暗号復号処理部からの要求に応じて提供する）。出力されたアクセス鍵は安全に暗号復号処理部に送信するために、暗号化されてａｋに記録するようにしても良い。

【００８８】

アクセス鍵生成部におけるアクセス鍵生成処理について、例を用いて説明する。

【００８９】

例えば、アクセスを許可するインデックスａｎとして、タイルグループインデックス「０－０－０」（図４Ｂ参照）を指定したとする。すると、入力されたコードストリーム鍵ｃｋ（ルートノードに対応する）から、タイルグループインデックス「０－０」に対応するタイルグループ鍵をハッシュ関数を用いて生成する。更に、生成されたタイルグループ「０－０」のタイルグループ鍵から、タイルグループ０－０－０のタイルグループ鍵を生成し、それをタイルグループ鍵０－０－０のアクセス鍵ａｋ（図１０）として出力する。

【００９０】

[暗号復号処理部]

先ず、実施形態における暗号復号処理部１４３と、アクセス鍵生成処理部１４２との大まかな動作を説明し、その後で、具体的な暗号復号処理部１４３の処理内容を説明することとする。暗号復号処理部１４３はインターネットに接続し得る一般のユーザが所有しているＰＣ、アクセス鍵生成処理部１４２は暗号化を解除するための認証サーバとして考えると分かりやすいので、それを前提にして説明する。

【００９１】

暗号化されたコードストリームｃ’を受信した暗号復号処理部（クライアントＰＣ）１４３は、非暗号化のタイルパートの符号データに基づいて画像を再現する。従って、再現できる画像の解像度は自ずと限られていることになる。このとき、その暗号復号処理部のユーザが、より高い解像度を再現できるよう望む場合、暗号化されているタイルパートから上位に遡って、要求するレベルのノードをユーザからの指示に従い決定する。このノードのレベル（タイルグループインデックスかタイルパートインデックス）をアクセス鍵生成処理部１４２（認証サーバ）にインデックスａｎとして要求する。この結果、アクセス鍵生成処理部１４２からは、要求したノードに対するアクセス鍵ａｋが送られてくるので、受信したアクセス鍵ａｋに基づき、その下位に向かう暗号を解除するための鍵群を生成する。そして、その鍵を用いて符号データの暗号化を解除し、復号を行なう。

【００９２】

なお、アクセス鍵生成処理部１４２としては、アクセス鍵ａｋを取得したい旨の要求をクライアント（復号処理部に対応する）から受信した場合、認証処理や課金等の処理を経て、そのアクセス鍵を提供することになるであろう。従って、このアクセス鍵生成処理部１４２をインターネットに認証サーバとして設置する場合、複数の暗号化処理部、複数の復号処理部を想定して設置する必要があり、必然、多数の画像を特定する情報と共に、それら個々の画像に対するコードストリーム鍵を登録できるようにしておく。そして、復号処理部１４３は、画像を特定する情報と暗号を解除するためのノードインデックスを通知することで、目的とする画像の目的とするノードレベルのアクセス鍵ａｋを得るようになる。アクセス鍵生成処理部１４２（認証サーバ）としては、１つの画像について、その画像を特定する情報（ＩＤやファイル名等）と、その画像のルートノードに対する１つのコードストリームだけ記憶していれば良いので、記憶管理する情報量も少なくできよう。

【００９３】

上記を踏まえ、以下、図１１を用いて本実施形態に適用される暗号復号処理部（機能）を説明する。

【００９４】

図１１に示すように、本実施形態における暗号復号処理部は、鍵行列生成部１１１、暗号復号部１１２、及び暗号化タイルパート判定部１１３から構成される。

【００９５】

まずはじめに、鍵行列生成部１１１の処理の詳細を説明する。鍵行列生成部１１１には、アクセス鍵生成処理部１４２に要求したタイルグループインデックス、或いはタイルパートインデックスに対するアクセス鍵ａｋが入力される。そして、入力されたアクセス鍵ａｋから、鍵行列ｋａ’（各ノード（タイル及びタイルパート）に対応する解読キー）を生成し、その生成された鍵行列ｋａ’を出力する。

【００９６】

ここで、鍵行列生成部１１１で実行される鍵行列生成処理について図１２を用いて、詳細に説明をする。図１２は鍵行列生成部１１１で実行される鍵行列生成処理を示すフローチャートである。

【００９７】

まず、ステップＳ１２１で入力されたアクセス鍵ａｋがタイルグループに対応するものか、或いはタイルパートに対応するものかが判定される。この判定のためには、図１０に示した「タイルパートインデックスかタイルグループインデックスかを示す情報」を利用する。判定結果がタイルグループインデックスの場合にはステップＳ１２２に進み、判定結果がタイルパートインデックスの場合にはステップＳ１２８に進む。

【００９８】

ステップＳ１２２（タイルグループインデックスの場合）では、パラメータｉ、及びパラメータｊを、図１０に示したアクセス鍵フォーマット中の「アクセス鍵値に対応するインデックス」に初期化する。パラメータｉは前述したツリー構造におけるレベルを示すインデックスであり、パラメータｊは前述した各レベルにおけるノードを表すインデックスである。即ち、ｉとｊの組み合わせ（ｉ，ｊ）はタイルグループインデックスである。

【００９９】

一方、タイルパートインデックスであると判断し、ステップＳ１２８に進んだ場合には、パラメータｍ、及びパラメータｎを、図１０に示したアクセス鍵フォーマット中の「アクセス鍵値に対応するインデックス」に初期化にする。ここで、パラメータｍはタイルインデックス、パラメータｎはタイルグループインデックスを示す。

【０１００】

その他の処理は、図６における鍵生成処理と同様の処理であるので詳細な説明は省略する。

【０１０１】

以上、説明したように、鍵行列生成処理により鍵行列ｋａ’が生成される。生成された鍵行列ｋａ’は暗号復号部１１２に入力される。

【０１０２】

次に、暗号化タイルパート判定部１１３の処理の詳細を説明する。暗号化タイルパート判定部１１３には、暗号化されたコードストリームｃ’が入力され、入力されたコードストリームｃ’からタイルパートが抽出され、抽出されたタイルパートが暗号化されているか否かが判定され、暗号化タイルパート情報ｔａ’が出力される。

【０１０３】

本実施形態における暗号化部分判定部１１３では、入力されたコードストリームｃ’中のタイルパートヘッダ部分を解析し、タイルパート部分に「タイルパートが暗号化されていることを示す情報」Ｉｎｆが記録されているか否かを調べる。判定された情報は、暗号化タイルパート情報ｔａ’として出力される。暗号化タイルパート情報ｔａ’の一例を図１３に示す。

【０１０４】

図１３は、画像全体が６４個のタイルから構成され、タイルパートの数の最大が５である場合の暗号化タイルパート情報ｔａ’の例を示す。図１３に示すように、暗号化タイルパート情報ｔａ’の各行はタイルに相当し、各列はタイルパートに相当する。行列の要素値としては、暗号化されていない場合には０を、暗号化されている場合には１を、存在しないタイルパートには２を記録する。

【０１０５】

次に、暗号復号部１１２の処理の詳細を説明する。暗号復号部１１２には、暗号化されたコードストリームｃ’、鍵行列ｋａ’、及び暗号化タイルパート情報ｔａ’が入力され、暗号化タイルパート情報ｔａ’に示されたコードストリームｃ’のタイルパートが、鍵行列ｋａ’に記録されているタイルパート鍵を用いて復号され、復号されたコードストリームｃ’が出力される。

【０１０６】

暗号化処理部１３では、暗号化タイルパート行列ｔａ’と鍵行列ｋａ’を比較し、暗号化タイルパート行列ｔａ’の要素値が１であるタイルパートに対して、鍵行列ｋａ’中の同じ座標に位置する鍵を用いて、コードストリームｃ中のタイルパートを暗号復号処理する。そして、コードストリームｃ’のタイルパートは、暗号復号処理されたタイルパートに置き換えられる。

【０１０７】

また、暗号復号処理したタイルパートは、タイルパートヘッダに記録されている、該タイルパートが暗号化されていることを示す為の情報Ｉｎｆを消去する。

【０１０８】

更に、ヘッダ部分は暗号復号処理せずにデータ部分だけを暗号復号処理するようにする。

【０１０９】

暗号復号処理の方法としては、暗号化処理部で実行した方法に対応する方法でなければならない。

【０１１０】

以上の様に、アクセス鍵に応じて、暗号化されたコードストリームｃ’が暗号復号され、暗号復号されたコードストリームは、暗号復号コードストリームｃ’’として出力される。

【０１１１】

従って、図１４における復号処理部１４３が、アクセス鍵生成処理部１４２からアクセス鍵ａｋを受信しないで、暗号化されたコードストリームｃ’を受信し復号処理したとしても、暗号化されていないタイルパートについては復号が成功

するだけとなり、予め許容された解像度以下の画像の再現までが可能となる。換言すれば、復号処理部１４３のユーザが、より鮮明な画像を望む場合には、アクセス鍵ａｋを取得し、再度復号化処理を行えば良いことになる。

【０１１２】

以上説明したように本第１の実施形態によれば、複数のタイル及び階層構造を有する画像データに対して、タイル及び階層構造毎に異なる暗号鍵を用いて暗号化した場合にも、複数の鍵を管理する必要がないようにすることが可能となる。更に、複数のタイル及び階層構造と、それらに対応する復号鍵を記録し、正しく復号処理を実行することか可能となる。

【０１１３】

なお、上記の実施形態でのタイルパートとは、ウェーブレット変換処理を行った際に生成される各周波数成分領域の集合単位とするものであったが、これに限定されるものではない。

【０１１４】

例えば、一般に画像の圧縮符号化では、ウェーブレット変換や直交変換等の周波数変換処理して得られたデータを量子化し、エントロピー符号化を施すが、量子化して得られた各係数値のビット単位のプレーン毎に符号化することを行う提案も既に幾つかなされており、これに適用させても良いからである。より具体的に説明するため、図１５を用いて説明する。

【０１１５】

図１５は、量子化した後の係数値のブロックを示している。図示では説明を単純化するため、４×４としているが勿論、これより大きくても構わないし、一般に、このサイズよりも大きなものとなる。座標（ｉ，ｊ）として表現したとき、図示は、（１，１）の係数値が「５」、（３，１）が「３」、（１、３）が「２」という値を持ち、それ以外は「０」となっている例を示している。この中で値が最も大きいものが「５」であり、バイナリー（２進）で表記すると「１０１」となる。つまり、図示の場合、全ての係数が３ビットで表現できるので、ビット２のプレーン、ビット１のプレーン、ビット０のプレーンの３つのプレーンがあれば十分に表現でき、ビットプレーン毎に符号化を行う。

【０１１６】

一方、データの重要度から見た場合、高位のビットほどその重要であるから、結局のところ、ビット２のプレーンがそのブロックの画質に支配的となり、以下、画質に与える影響の大きな順は、ビット１のプレーン、ビット０のプレーンとなる。これは、ちょうど、先に説明したウェーブレット変換を複数回行った際の、最も低周波成分の係数値（ＬＬ成分）が、ビット２のプレーンであり、最も高周波成分の係数の集合｛ＬＨ１＋ＨＬ１＋ＨＨ１｝がビット０のプレーンに対応するのと同様の意味を持つことに他ならない。

【０１１７】

一方、周波数変換し、量子化した後の値の最大値によって、符号化する対象のプレーンの数が決定されるわけであるから、そのプレーンの数は個々のタイルによって異なる。仮に、固定の量子化ステップで量子化し、その時に取り得る値が０乃至６３であるとしたとき、最大で６つのプレーン（ビット０～５のプレーン）が発生し得ることになる。図１５は、このような状況において、たまたま全ての係数が３ビット（ビット０乃至２）以内で表現でき、ビット３乃至５のプレーンは生成する必要はない。すなわち、使用していないビットプレーンについては、そのデータが存在しなくても良いから、先に説明した図８に示した暗号化タイルパート行列内に「２」が格納される。

【０１１８】

従って、タイルパートは、上記のように、符号化する際に用いたビットプレーンの数を割り当て、最も上位のビットプレーンに対して小さなタイルパートのインデックスを割り当てることでも、全く同様の効果が期待できる。或いは、符号化する際に用いたビットプレーンのいくつかのまとまりをレイヤとし、最も上位のレイヤに対して小さなタイルパートのインデックスを割り当てるようにしてもよい。

【０１１９】

また、画像を符号化する際、原画像中のＭ×Ｎ画素で表現される部分画像（プレシンクト）を更に幾つかに分割し、個々の分割領域をタイルパートとして定義しても構わない。

【０１２０】

さらに、複数の成分（輝度成分や、色成分など）から構成される画像を符号化する際、所定の成分（例えば、輝度値）をタイルパートとして定義しても構わない。

【０１２１】

以上を簡単にまとめると、実施形態における暗号化対象の指定とその暗号化処理は２通り存在することになる。

【０１２２】

１つ目は、或るタイルグループを暗号化対象として指定したとき、そのタイルグループに属する下位のレベルのタイルグループ、最終的には指定されたタイルグループに属する全タイルが暗号化対象として設定される。そして、ルート（レベル０）のタイルグループに対して生成された暗号化キーから派生して生成されたキーを用いて、暗号化対象のタイルデータが暗号化される。

【０１２３】

この結果、暗号化キーとしては１つで済み、尚且つ、所望とするタイルグループに属するタイルについて暗号化させることができる。

【０１２４】

２つ目は、或るタイルパートに対して暗号化対象として指定したとき、その指定されたタイルパートのインデックス以上のインデックスを有するタイルパートを暗号化させることができることである。換言すれば、暗号化対象として指定したタイルパートより小さいインデックスを有するタイルパートについては非暗号化となるので、解像度の低い画像については無条件に再現できるものの、それを越える解像度について、解読キーを有しない限り不可にできる。

【０１２５】

[第２の実施形態]

第１の実施形態においては、図１において鍵行列指定部１２と暗号化部１３を分離させ、鍵行列指定部１２の出力である鍵行列ｋａを暗号化部１３に入力するようにしていた。また、図１１における鍵行列ｋａ’も同様である。鍵行列ｋａ、及び鍵行列ｋａ’の大きさは画像を構成するタイル数とタイルパートの最大値

によって決定する。よって、多くのタイルを有する画像であったり、タイルパートの最大値が場合には、鍵行列ｋａ、及び鍵行列ｋａ’の大きさが大きくなってしまうことがある。

【０１２６】

しかしながら本発明は、これに限定されることなく、鍵行列生成部１２、及び鍵行列生成部１１１は必ずしも鍵行列ｋａ、及び鍵行列ａ’を全画像分まとめて出力する必要はない。ひとつの鍵が生成される度に、生成された鍵を暗号化部１３、或いは暗号復号部１１２に出力するようにするようにすることも可能である。このようにすることによって、鍵のために必要とされるメモリ量を小さくすることが可能となる。

【０１２７】

以上説明したように本実施形態によれば、複数のタイル及び階層構造を有する画像データに対して、タイル及び階層構造毎に異なる暗号鍵を用いて暗号化した場合にも、複数の鍵を管理する必要がないようにすることが可能となる。更に、複数のタイル及び階層構造と、それらに対応する復号鍵を記録し、正しく復号処理を実行することか可能となる。

【０１２８】

［第３の実施形態］

第１の実施形態においては、タイルグループ鍵、及びタイル鍵の生成のために（式２）を用い、タイルパート鍵の生成のために（式３）を用いるようにした。

【０１２９】

しかしながら、本発明はこれに限定されることはなく、鍵生成のために種々の処理を行うことが可能である。例えば、図６におけるＳ６３において、タイル鍵を、その親のタイル鍵のハッシュ値として（式２’）の様に算出しても良い。

Ｋ（ｊ＋１）＝Ｈ（Ｋ（ｊ））　　（式２’）

ここで、ｊはタイルインデックスである。また、図６におけるＳ６９において、タイルパート鍵を、タイル鍵とタイルパートインデックスのハッシュ値として（式３’）の様に算出しても良い。

Ｋ（ｍ、ｎ）＝Ｈ（Ｋ（ｍ）、ｎ）　　（式３’）

ここで、ｍはタイルインデックス、ｎはタイルパートインデックスである。

【０１３０】

このように生成された鍵のツリー構造を図１６に示す。図１６は、４つのタイルと、夫々のタイルが３つのタイルパートから構成されるコードストリームｃに対応する鍵を、前記（式２’）及び（式３’）を用いて生成した際の鍵のツリー構造を示す図である。

【０１３１】

以上のような処理とすることにより、各々タイルに対する鍵は親のノードに対応するタイル鍵からハッシュ関数だけによって生成することができる。例えば、タイルインデックス２とタイルインデックス３に対応するタイルへのアクセスを許可するような場合に、第１の実施形態においては、アクセス鍵生成処理部において、タイルインデックス２とタイルインデックス３に対応する２つのタイル鍵を生成し、暗号復号部に送信しなければならなかった。一方で、本実施形態においては、アクセス鍵生成処理部においてタイルインデックス２に対応する１つのタイル鍵だけを生成し、暗号復号部に送信するようにすればよく、効率的である。

【０１３２】

また、各々のタイルパートに対する鍵は親のノードに対応するタイル鍵と、当該タイルパートのタイルパートインデックスとから、ハッシュ関数を用いて算出できる。例えば、第１の実施形態では、タイルパート１に対応するタイルパートだけへのアクセスを許可することは困難であった。これは、タイルパート１へアクセスを許可することは、同時にその子ノードに対応するタイルパート０への許可をアクセスすることになったからである。一方で、本実施形態においては、タイルパート１に対応するタイルパート鍵は、その親ノードに対応するタイル鍵と、当該タイルパートインデックス１から生成できるため、より柔軟なアクセス制御を実現可能である。

【０１３３】

更に、図６のおけるＳ６３において、タイル鍵を（式２’）のように生成し、Ｓ６９において、タイルパート鍵を（式３）のように生成したり、或いは、Ｓ６

３において、タイル鍵を（式２）のように生成し、Ｓ６９において、タイルパート鍵を（式３’）のように生成するようにすることも可能であることは明らかである。

【０１３４】

［第４の実施形態］

第３の実施形態においては、タイルパート鍵が、親ノードに対応するタイル鍵と、当該タイルパートに対応するタイルパートインデックスとから生成される例を説明した。更に、本実施の形態においては、タイルパート鍵がグループ化されて生成される例を説明する。

【０１３５】

本実施形態におけるタイルパート鍵生成処理を図１７を用いて説明する。図１７は本実施形態におけるタイルパート鍵生成処理を説明するフローチャートである。図６に示したフローチャートにおけるＳ６８からＳ７４までの処理を、図１７に示す処理に置き換えるようにすればよい。

【０１３６】

まず、ステップＳ１７１において、パラメータｉ及びｊが“０”に初期化される。パラメータｉはツリー構造におけるレベルを示すインデックスであり、パラメータｊは各レベルにおけるノードを表すインデックスである。特に、ｉとｊのくみあわせ（ｉ、ｊ）をタイルパートグループインデックスと呼ぶ。

【０１３７】

次のステップＳ１７２では、タイルパートグループインデックス（ｉ，ｊ）のタイルパートグループ鍵が生成される。タイルパートグループ鍵は、その親のタイルパートグループ鍵、及びタイルパートグループインデックス（ｉ，ｊ）のハッシュ値として式（４）のように算出される。

Ｋ（ｉ，ｊ）＝Ｈ（Ｋ（ｉ－１、ｋ），ｉ，ｊ）　　（式４）

ここで、ｋはタイルパートグループ（ｉ，ｊ）の親ノードに対応するノードを表すインデックスである。即ち、親ノードに対応するタイルパートグループ鍵Ｋ（ｉ－１，ｋ）と、生成するタイルパートグループ鍵に対応するノードのタイルパートグループインデックス（ｉ，ｊ）とからタイルパートグループ鍵が生成さ

れる。しかしながら、本発明はこれに限定されることなく、親ノードに対応する鍵と、生成するタイルパートグループ鍵に対応するノードに含まれるタイルパートインデックスとからタイルパートグループ鍵を生成するようにしてもよい。

【０１３８】

例えば、生成するタイルパートグループに対応するノードから順に木をたどり、タイルパートに対応するノードを調べ、当該タイルパートのタイルパートインデックを用いるようにすれば良い。要するに、上位ノード（ルートノード側にあるノード）に対する鍵ｃｋと、その下位（下層）方向にあるノードのインデックスに基づいて、下位にあるノードの鍵を派生することを順に繰り返すことになる。

【０１３９】

ここで、（式４）を用いて生成されたタイルパートグループ鍵のうち、最も子ノードに位置するレベルの鍵はタイルパート鍵である。タイルパート鍵の場合には、生成した鍵を鍵行列ｋａに記録される。

【０１４０】

ステップＳ１７３では、レベルｉにおいて全てのノードに対応するタイルパートグループ鍵が生成されたか否かが判定される。判定結果が真の場合はステップＳ１７５に進み、判定結果が偽の場合はステップＳ１７４に進む。

【０１４１】

ステップＳ１７４では、パラメータｊが１だけ増やされ、その後ステップＳ１７２が再度処理される。つまり、パラメータｉで示されるレベルに属する全タイルパートグループについて鍵が生成されることになる。

【０１４２】

一方、パラメータｉで示されるレベルに対するタイルパートグループ鍵が生成されると、処理はステップＳ１７５に進み、全てのレベルが処理されたか否かが判定される。判定結果が真の場合は処理を終了する。判定結果が偽の場合はステップＳ１７６に進んで、次のレベルの処理を行うべく、パラメータｉを１だけ増加させ、ステップＳ１７２以降の処理を繰り返す。

【０１４３】

以上のように、タイルパートをグループ化して鍵行列を生成することによって、複数のタイルパートに対するアクセス制御をする際にはタイルパートグループ鍵をアクセス鍵生成処理部で生成するようにすればよく、効率的にアクセス制御することが可能となる。

【０１４４】

また以上説明した実施形態における、暗号化処理部１４１、アクセス鍵生成処理部１４２、更には、復号処理部１４３は、それぞれパーソナルコンピュータ等の情報処理装置でもって実現できるし、その機能を実現する手順としての方法の発明として捉えることができる。また、コンピュータにより実現できるわけであるから、本発明はそれぞれの装置で実行されるコンピュータプログラム、更には、そのコンピュータプログラムを格納し、コンピュータが読み込めるＣＤＲＯＭ等のコンピュータ可読記憶媒体にも適用できるのは明らかであろう。

【０１４５】

従って、上記実施形態に係る実施態様を列挙すると、次の通りである。すなわち、暗号化処理部１４１としての情報処理方法及び装置、並びにコンピュータプログラム及びコンピュータ可読記憶媒体は、次のようになる。

【０１４６】

［実施態様１］　タイル単位に圧縮符号化された画像データを入力し、暗号化する情報処理方法であって、

隣接する複数のタイルで１つのタイルグループを構成し、更に、隣接するタイルグループで１つの更なるタイルグループを構成することを繰り返すことで、タイルグループの階層構造を定義し、

符号化データで表現される画像全体から、最上位階層の暗号化鍵情報を生成し、

前記階層構造中の、上位に位置するタイルグループに対して生成された暗号化鍵情報に基づき、下位層に位置するタイルグループ或いはタイルに対する暗号化鍵情報を生成することを、末端に位置するタイルまで行ない、

前記タイルグループのツリー構造中の、所望とする階層の所望とするタイルグループを暗号化対象とする指定入力が与えられた場合、当該指定入力されたタイ

ルグループに属する下位層の末端に位置するタイルに対して暗号化を行うよう設定し、

暗号化を行うよう設定された個々のタイルに対し、当該タイルに対して生成された暗号化キーを用いて暗号化処理を行ない、当該暗号化した符号化データ及び暗号化されていないタイルの符号化データを出力する

ことを特徴とする情報処理方法。

【０１４７】

［実施態様２］　前記暗号化鍵情報は、上位階層から下位階層に向かう一方向性を有する関数を用いて生成することを特徴とする実施態様１に記載の情報処理方法。

【０１４８】

［実施態様３］　前記関数は、下位階層にあるタイルグループもしくはタイルの座標位置情報をパラメータとして鍵情報を生成することを特徴とする実施態様２に記載の情報処理方法。

【０１４９】

［実施態様４］　前記最上位階層の暗号化鍵情報は、所定のインターネット上の認証用サーバに出力することを特徴とする実施態様１に記載の情報処理方法。

【０１５０】

［実施態様５］　更に、入力した符号化データを、タイル及びタイルグループの階層構造として表示する工程を備え、

前記所望とする階層の所望とするタイルグループは、前記表示工程での表示された階層構造から指定することを特徴とする実施態様１に記載の情報処理方法。

【０１５１】

［実施態様６］　タイル単位に圧縮符号化されたデータを入力し、暗号化する情報処理装置であって、

隣接する複数のタイルで１つのタイルグループを構成し、更に、隣接するタイルグループで１つの更なるタイルグループを構成することを繰り返すことで、タイルグループの階層構造を定義する手段と、

符号化データで表現される画像全体から、最上位階層の暗号化鍵情報を生成す

る手段と、

前記階層構造中の、上位に位置するタイルグループに対して生成された暗号化鍵情報に基づき、下位層に位置するタイルグループ或いはタイルに対する暗号化鍵情報を生成することを、末端に位置するタイルまで行なう手段と、

前記タイルグループのツリー構造中の、所望とする階層の所望とするタイルグループを暗号化対象とする指定入力が与えられた場合、当該指定入力されたタイルグループに属する下位層の末端に位置するタイルに対して暗号化を行うよう設定する手段と、

暗号化を行うよう設定された個々のタイルに対し、当該タイルに対して生成された暗号化キーを用いて暗号化処理を行ない、当該暗号化した符号化データ及び暗号化されていないタイルの符号化データを出力する手段と

を備えることを特徴とする情報処理装置。

【０１５２】

［実施態様７］　コンピュータが読み込み実行することで、タイル単位に圧縮符号化されたデータを入力し、暗号化する情報処理装置として機能するコンピュータプログラムであって、

隣接する複数のタイルで１つのタイルグループを構成し、更に、隣接するタイルグループで１つの更なるタイルグループを構成することを繰り返すことで、タイルグループの階層構造を定義する手段と、

符号化データで表現される画像全体から、最上位階層の暗号化鍵情報を生成する手段と、

前記階層構造中の、上位に位置するタイルグループに対して生成された暗号化鍵情報に基づき、下位層に位置するタイルグループ或いはタイルに対する暗号化鍵情報を生成することを、末端に位置するタイルまで行なう手段と、

前記タイルグループのツリー構造中の、所望とする階層の所望とするタイルグループを暗号化対象とする指定入力が与えられた場合、当該指定入力されたタイルグループに属する下位層の末端に位置するタイルに対して暗号化を行うよう設定する手段と、

暗号化を行うよう設定された個々のタイルに対し、当該タイルに対して生成さ

れた暗号化キーを用いて暗号化処理を行ない、当該暗号化した符号化データ及び暗号化されていないタイルの符号化データを出力する手段と

して機能することを特徴とするコンピュータプログラム。

【０１５３】

［実施態様８］　実施態様７に記載のコンピュータプログラムを格納することを特徴とするコンピュータ可読記憶媒体。

【０１５４】

また、復号処理部１４３としての情報処理方法及び装置、並びにコンピュータプログラム及びコンピュータ可読記憶媒体は、次のようになる。

【０１５５】

［実施態様９］　暗号化／非暗号化されたタイル単位の符号化データが混在した情報を入力し、画像を再現する情報処理方法であって、

入力した情報に基づき、隣接する複数のタイルで１つのタイルグループを構成し、更に、隣接するタイルグループで１つの更なるタイルグループを構成することを繰り返すことで、タイルグループの階層構造を定義し、

暗号化されたタイルを包含する所望とする上位のタイルグループに対する、暗号解除を行うための鍵情報を入力し、

入力した鍵情報に基づき、当該鍵情報が示すタイルグループの下位層の鍵情報を生成することを、末端のタイルまで行い、

生成された各タイルに対する鍵情報を用いて、暗号化された各タイルの符号化データの暗号化を解除し、復号する

ことを特徴とする情報処理方法。

【０１５６】

［実施態様１０］　暗号化／非暗号化されたタイル単位の符号化データが混在した情報を入力し、画像を再現する情報処理装置であって、

入力した情報に基づき、隣接する複数のタイルで１つのタイルグループを構成し、更に、隣接するタイルグループで１つの更なるタイルグループを構成することを繰り返すことで、タイルグループの階層構造を定義する手段と、

暗号化されたタイルを包含する所望とする上位のタイルグループに対する、暗

号解除を行うための鍵情報を入力する手段と、

入力した鍵情報に基づき、当該鍵情報が示すタイルグループの下位層の鍵情報を生成することを、末端のタイルまで行う手段と、

生成された各タイルに対する鍵情報を用いて、暗号化された各タイルの符号化データの暗号化を解除し、復号する手段と

を備えることを特徴とする情報処理装置。

【０１５７】

［実施態様１１］　コンピュータが読み込み実行することで、暗号化／非暗号化されたタイル単位の符号化データが混在した情報を入力し、画像を再現する情報処理装置として機能するコンピュータプログラムであって、

入力した情報に基づき、隣接する複数のタイルで１つのタイルグループを構成し、更に、隣接するタイルグループで１つの更なるタイルグループを構成することを繰り返すことで、タイルグループの階層構造を定義する手段と、

暗号化されたタイルを包含する所望とする上位のタイルグループに対する、暗号解除を行うための鍵情報を入力する手段と、

入力した鍵情報に基づき、当該鍵情報が示すタイルグループの下位層の鍵情報を生成することを、末端のタイルまで行う手段と、

生成された各タイルに対する鍵情報を用いて、暗号化された各タイルの符号化データの暗号化を解除し、復号する手段と

して機能することを特徴とするコンピュータプログラム。

【０１５８】

［実施態様１２］　実施態様１１に記載のコンピュータプログラムを格納することを特徴とするコンピュータ可読記憶媒体。

【０１５９】

更に、アクセス鍵生成処理部１４２としてのサーバ及びその制御方法、並びにコンピュータプログラム及びコンピュータ可読記憶媒体は、次のようになる。

【０１６０】

［実施態様１３］　暗号化／非暗号化されたタイル単位の符号化データが混在した画像のための暗号解除鍵を提供するネットワークに接続されるサーバの処理

方法であって、

隣接する複数のタイルで１つのタイルグループを構成し、更に、隣接するタイルグループで１つの更なるタイルグループを構成することを繰り返す階層構造を有する画像の最上位に位置する基本解除鍵情報を記憶し、

解除させたい階層中のタイルグループを指定する情報を前記ネットワーク上のクライアントから受信したとき、指定された階層の指定されたタイルグループに到達するまで、前記基本解除鍵から下位層に向かって順次解除鍵情報を派生し、該当するタイルグループに対する解除鍵情報が生成された場合に、当該解除鍵情報を前記クライアントに通知する

ことを特徴とするサーバの処理方法。

【０１６１】

［実施態様１４］　暗号化／非暗号化されたタイル単位の符号化データが混在した画像のための暗号解除鍵を提供するネットワークに接続されるサーバであって、

隣接する複数のタイルで１つのタイルグループを構成し、更に、隣接するタイルグループで１つの更なるタイルグループを構成することを繰り返す階層構造を有する画像の最上位に位置する基本解除鍵情報を記憶する手段と、

解除させたい階層中のタイルグループを指定する情報を前記ネットワーク上のクライアントから受信したとき、指定された階層の指定されたタイルグループに到達するまで、前記基本解除鍵から下位層に向かって順次解除鍵情報を派生し、該当するタイルグループに対する解除鍵情報が生成された場合に、当該解除鍵情報を前記クライアントに通知する手段と

を備えることを特徴とするサーバ。

【０１６２】

［実施態様１５］　コンピュータが読み込み実行することで、暗号化／非暗号化されたタイル単位の符号化データが混在した画像のための暗号解除鍵を提供するネットワークに接続されるサーバとして機能するコンピュータプログラムであって、

隣接する複数のタイルで１つのタイルグループを構成し、更に、隣接するタイ

ルグループで１つの更なるタイルグループを構成することを繰り返す階層構造を有する画像の最上位に位置する基本解除鍵情報を記憶する手段と、

解除させたい階層中のタイルグループを指定する情報を前記ネットワーク上のクライアントから受信したとき、指定された階層の指定されたタイルグループに到達するまで、前記基本解除鍵から下位層に向かって順次解除鍵情報を派生し、該当するタイルグループに対する解除鍵情報が生成された場合に、当該解除鍵情報を前記クライアントに通知する手段と

して機能することを特徴とするコンピュータプログラム。

【０１６３】

［実施態様１６］　実施態様１５に記載のコンピュータプログラムを格納することを特徴とするコンピュータ可読記憶媒体。

【０１６４】

【発明の効果】

以上説明したように本発明によれば、複数のタイル及び階層構造を有する画像データに対して、タイル及び階層構造毎に異なる暗号鍵を用いて暗号化した場合にも、複数の鍵を管理する必要がないようにすることが可能となる。

【図面の簡単な説明】

【図１】

本実施形態における暗号処理部のブロック構成図である。

【図２】

本実施形態におけるタイル及びタイルパートを示す図である。

【図３】

本実施形態におけるタイルグループ化を説明するための図である。

【図４Ａ】

第１の実施形態におけるタイルパート、及びタイルグループのツリー構造を示す図である。

【図４Ｂ】

図４Ａのツリー構造をタイルインデックス、タイルパートインデックスで示すツリー構造図である。

【図５】

本実施形態における暗号化対象タイルパート情報を説明する図である。

【図６】

本実施形態における鍵行列生成処理のフローチャートである。

【図７】

本実施形態における鍵行列の構造を示す図である。

【図８】

本実施形態における暗号化タイルパート行列の一例を示す図である。

【図９】

本実施形態におけるアクセス鍵生成処理部のブロック構成図である。

【図１０】

本実施形態におけるアクセス鍵のフォーマットを示す図である。

【図１１】

本実施形態における復号処理部のブロック構成図である。

【図１２】

本実施形態における鍵行列生成処理を説明する図である。

【図１３】

本実施形態における暗号化タイルパート情報の一例を示す図である。

【図１４】

本実施形態におけるシステムの全体構成図である。

【図１５】

タイルパートの他の形態を示す図である。

【図１６】

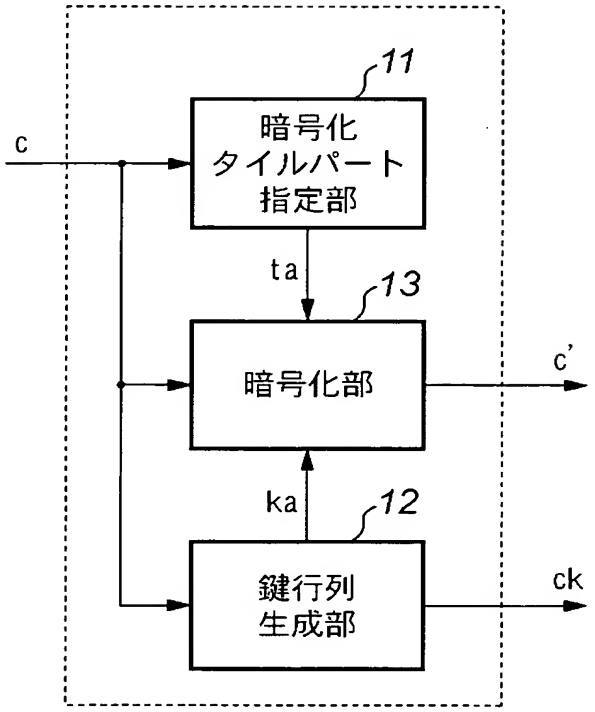
第３の実施形態におけるタイルパート、及びタイルグループのツリー構造を示す図である。

【図１７】

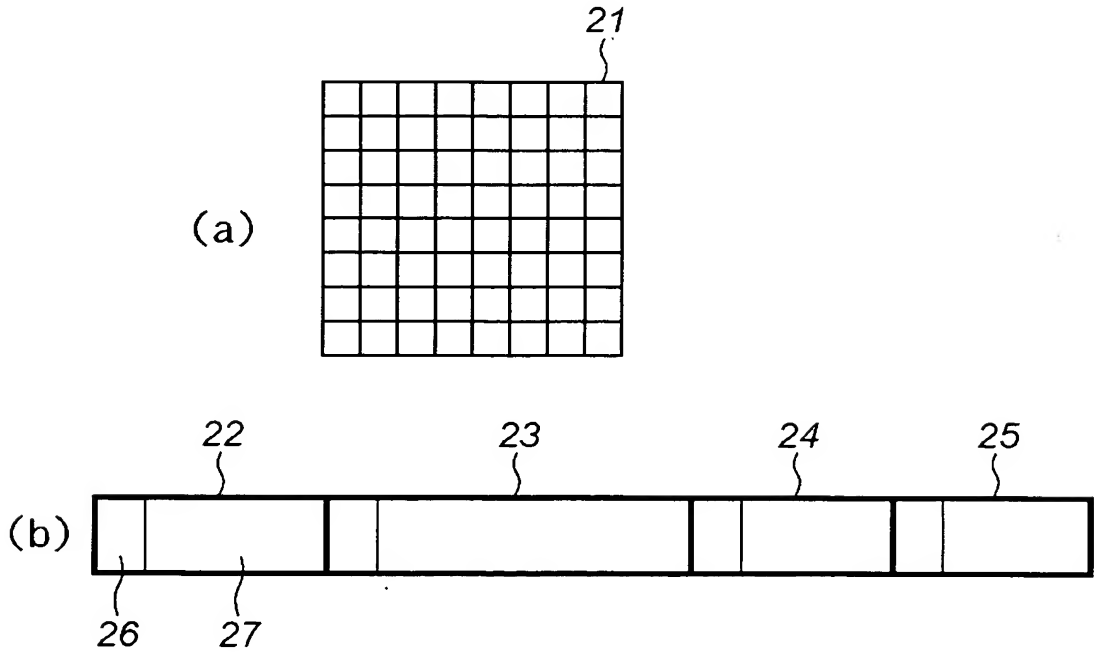
第４の実施形態における処理の一部分を示すフローチャートである。

【書類名】　図面

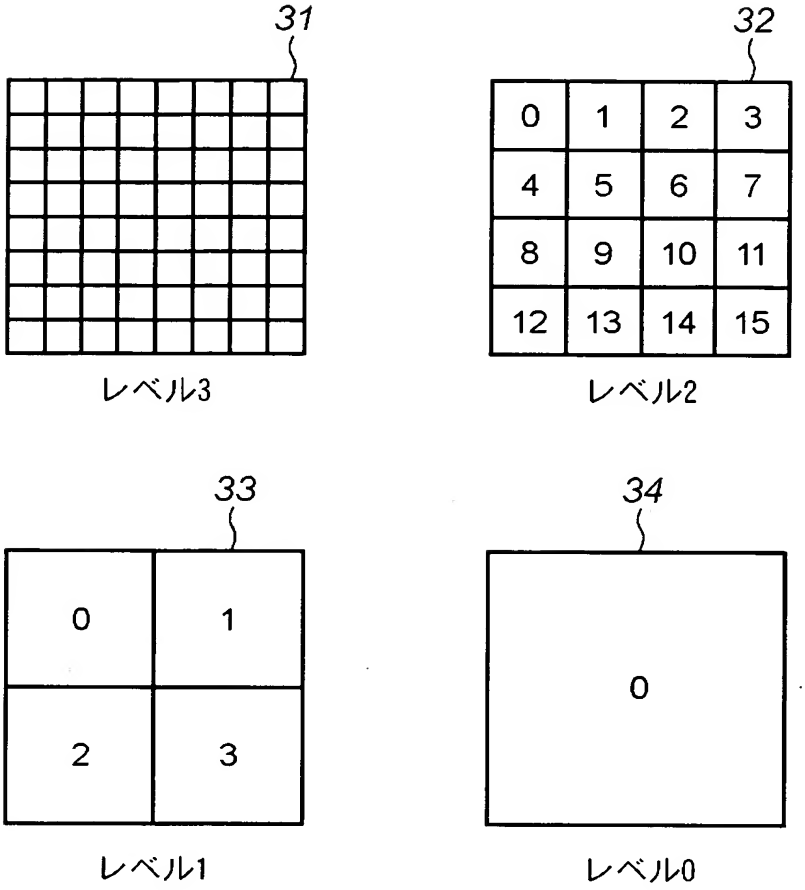
【図１】


11
暗号化
タイルパート
指定部
c
ta
13
暗号化部
c'
ka
12
鍵行列
生成部
ck

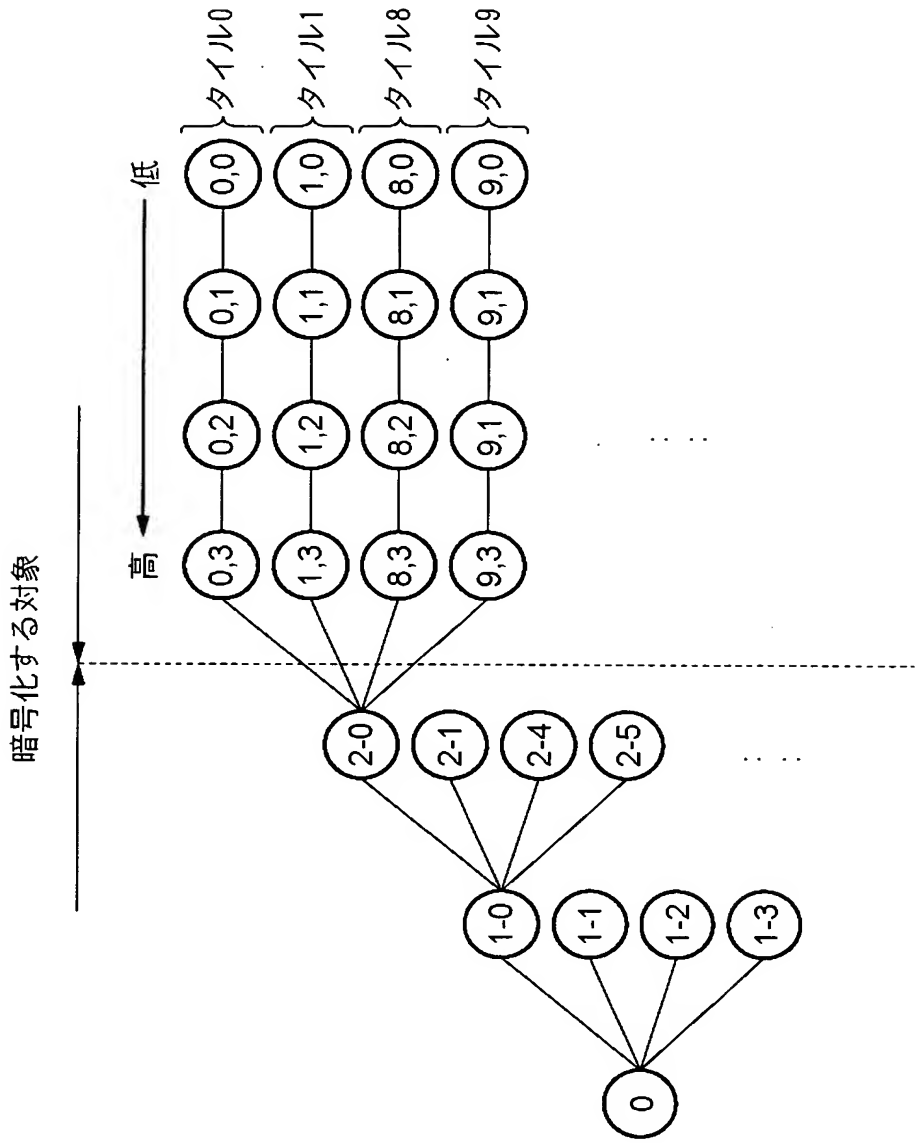
【図２】


21
(a)
22
23
24
25
(b)
26
27

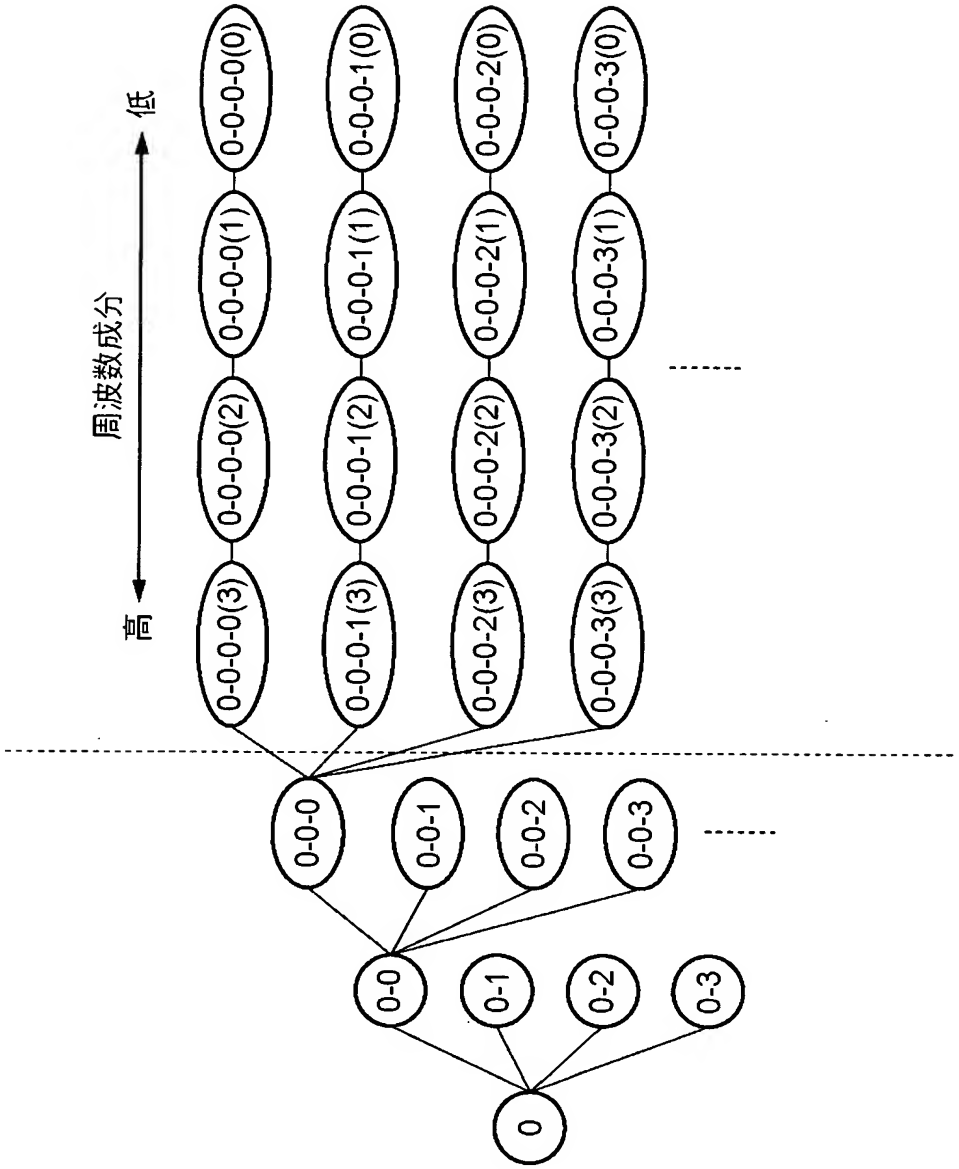
【図３】


31
32
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
レベル3
レベル2
33
34
0
1
2
3
0
レベル1
レベル0

【図４Ａ】


タイル0
タイル1
タイル8
タイル9
低
高
0,0
1,0
8,0
9,0
0,1
1,1
8,1
9,1
0,2
1,2
8,2
9,1
0,3
1,3
8,3
9,3
暗号化する対象
2-0
2-1
2-4
2-5
1-0
1-1
1-2
1-3
0

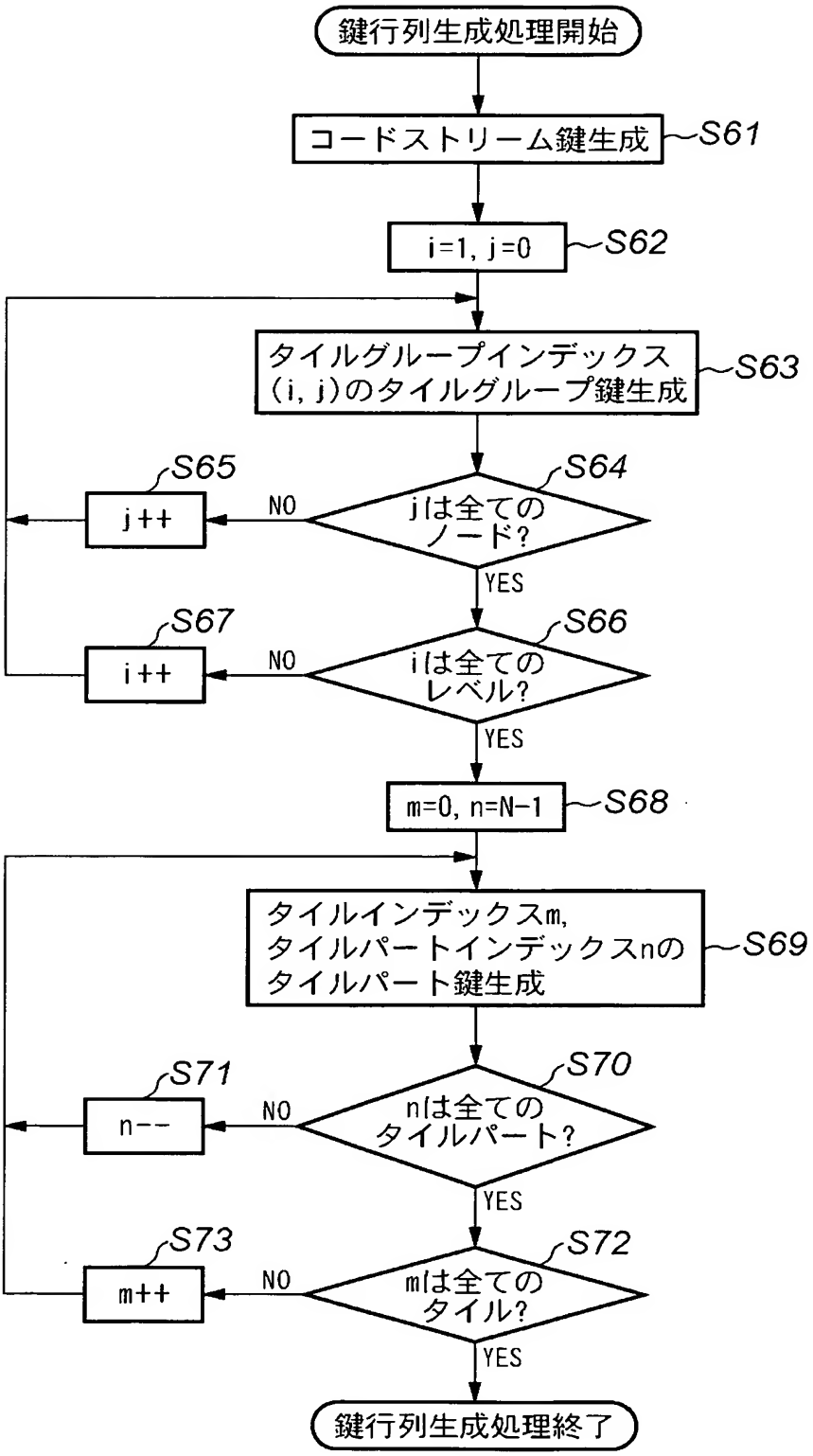
【図４Ｂ】


低
周波数成分
高
0-0-0-0(0)
0-0-0-0(1)
0-0-0-0(2)
0-0-0-0(3)
0-0-0-1(0)
0-0-0-1(1)
0-0-0-1(2)
0-0-0-1(3)
0-0-0-2(0)
0-0-0-2(1)
0-0-0-2(2)
0-0-0-2(3)
0-0-0-3(0)
0-0-0-3(1)
0-0-0-3(2)
0-0-0-3(3)
0-0-0
0-0-1
0-0-2
0-0-3
0-0
0-1
0-2
0-3
0

【図５】

タイルインデックス	暗号化されるタイルパートインデックスの最小値
0	0
1	2
3	3
4	1
5	0
:	:
62	3
63	1

【図６】


鍵行列生成処理開始
コードストリーム鍵生成
S61
i=1, j=0
S62
タイルグループインデックス(i, j)のタイルグループ鍵生成
S63
S64
jは全てのノード?
NO
S65
j++
YES
S66
iは全てのレベル?
NO
S67
i++
YES
m=0, n=N-1
S68
タイルインデックスm,タイルパートインデックスnのタイルパート鍵生成
S69
S70
nは全てのタイルパート?
NO
S71
n--
YES
S72
mは全てのタイル?
NO
S73
m++
YES
鍵行列生成処理終了

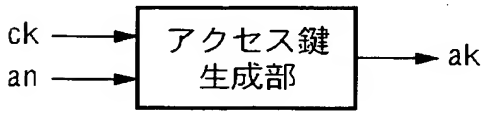
【図７】

	0	1	2	3	4	5
0						
1						
3						
4						
5						
:						
62						
63						

【図８】

	0	1	2	3	4	5
0	1	1	1	1	1	1
1	0	1	1	1	2	2
3	0	0	0	1	1	2
4	0	1	1	1	1	2
5	1	1	1	1	2	2
:	:	:	:	:	:	:
62	0	0	0	1	1	2
63	0	1	1	1	2	2

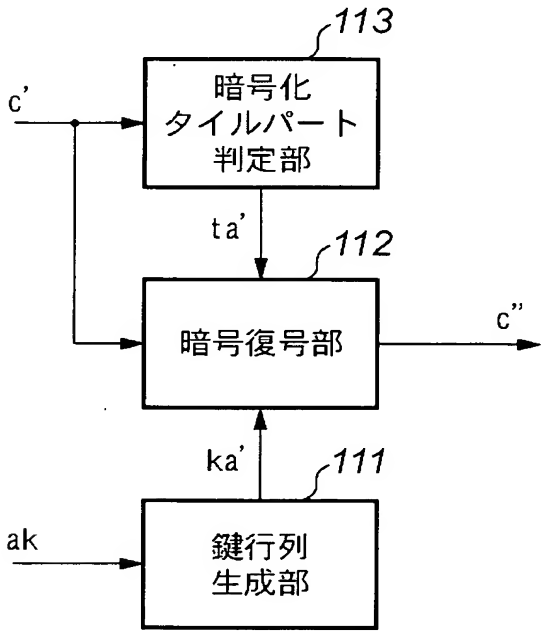
【図９】



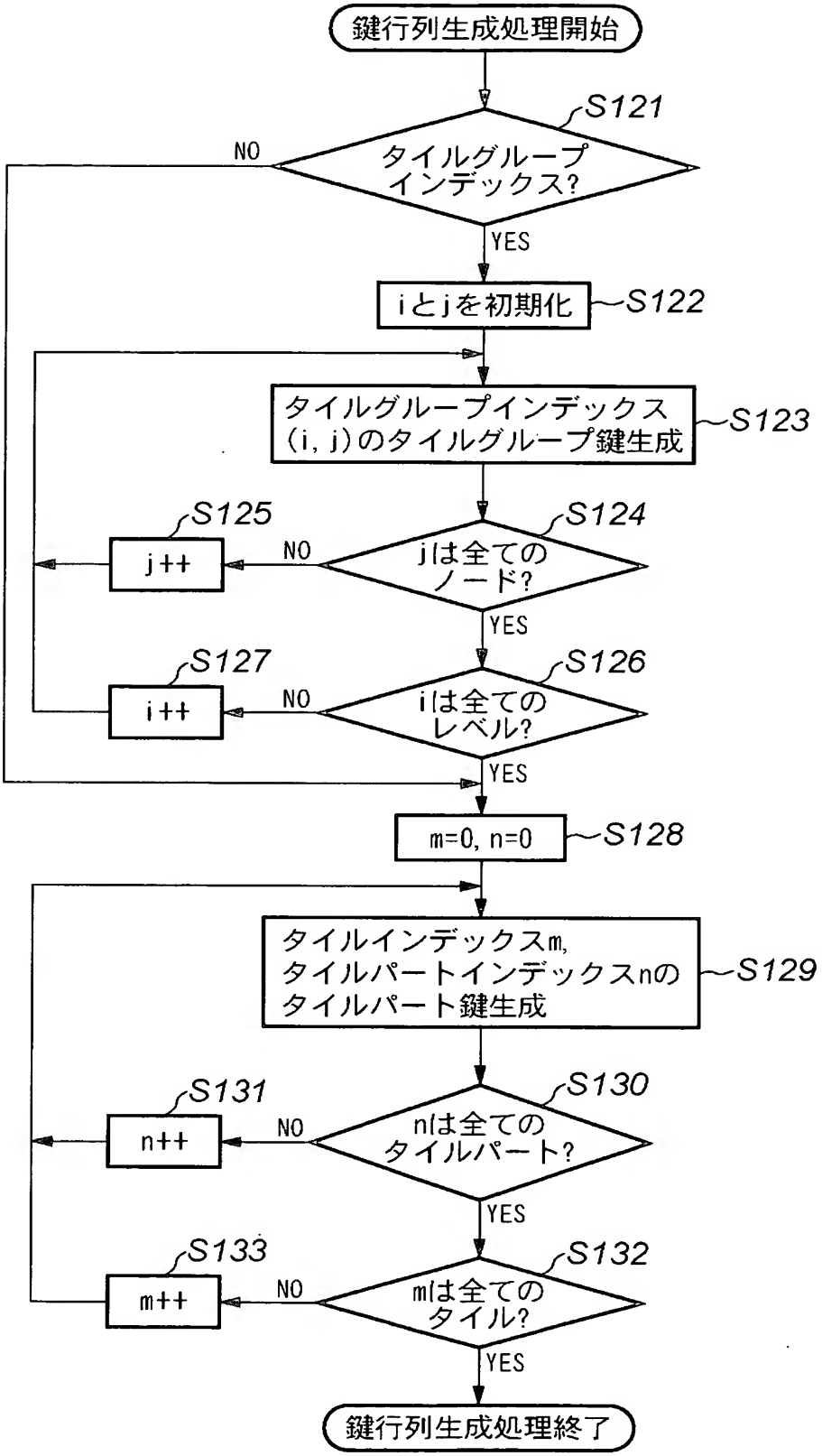
【図１０】

アクセス鍵値
アクセス鍵値に対応するインデックス
タイルパートインデックスかタイルグループインデックスかを示す情報

【図１１】



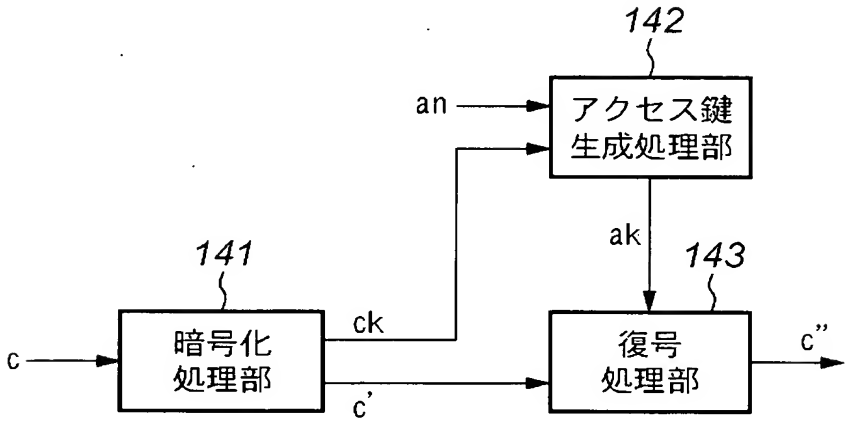
【図１２】


鍵行列生成処理開始
S121
タイルグループ
インデックス?
NO
YES
iとjを初期化
S122
タイルグループインデックス
(i, j)のタイルグループ鍵生成
S123
S125
j++
NO
S124
jは全ての
ノード?
YES
S127
i++
NO
S126
iは全ての
レベル?
YES
m=0, n=0
S128
タイルインデックスm,
タイルパートインデックスnの
タイルパート鍵生成
S129
S131
n++
NO
S130
nは全ての
タイルパート?
YES
S133
m++
NO
S132
mは全ての
タイル?
YES
鍵行列生成処理終了

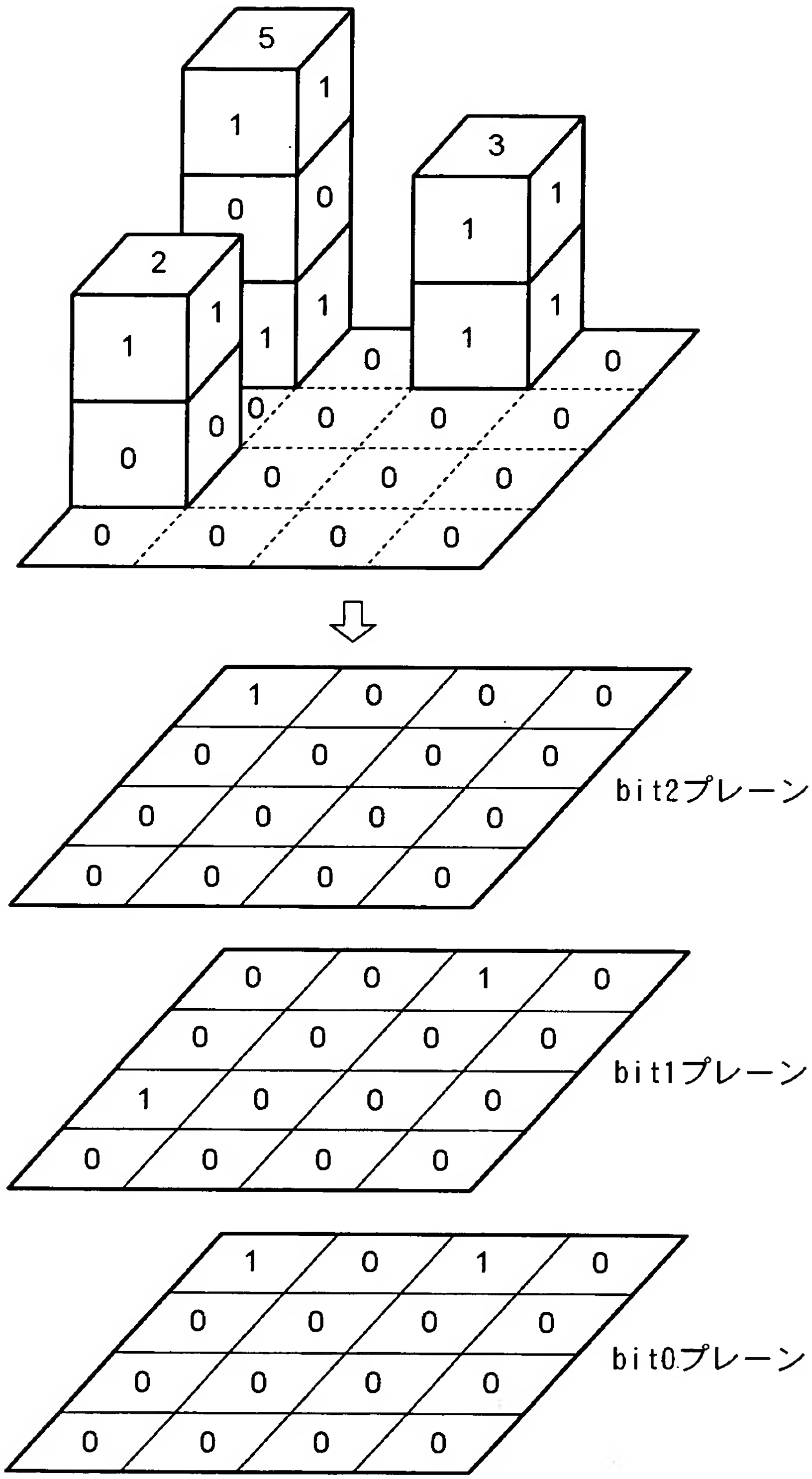
【図１３】

	0	1	2	3	4	5
0	1	1	1	1	1	1
1	0	0	1	1	2	2
2	0	0	0	1	1	2
3	0	1	1	1	1	2
4	1	1	1	1	2	2
:	:	:	:	:	:	:
62	0	0	0	1	1	2
63	0	1	1	1	2	2

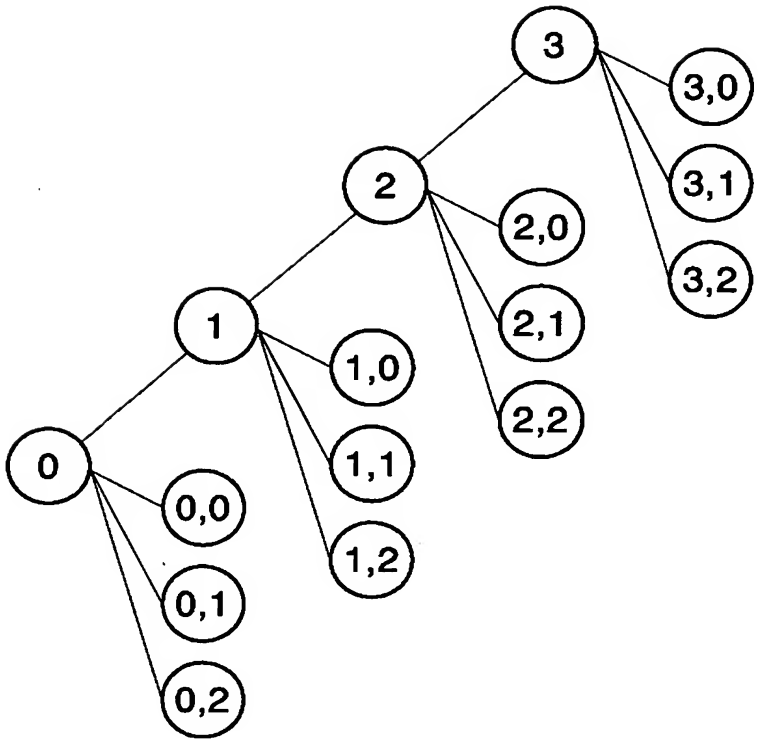
【図１４】



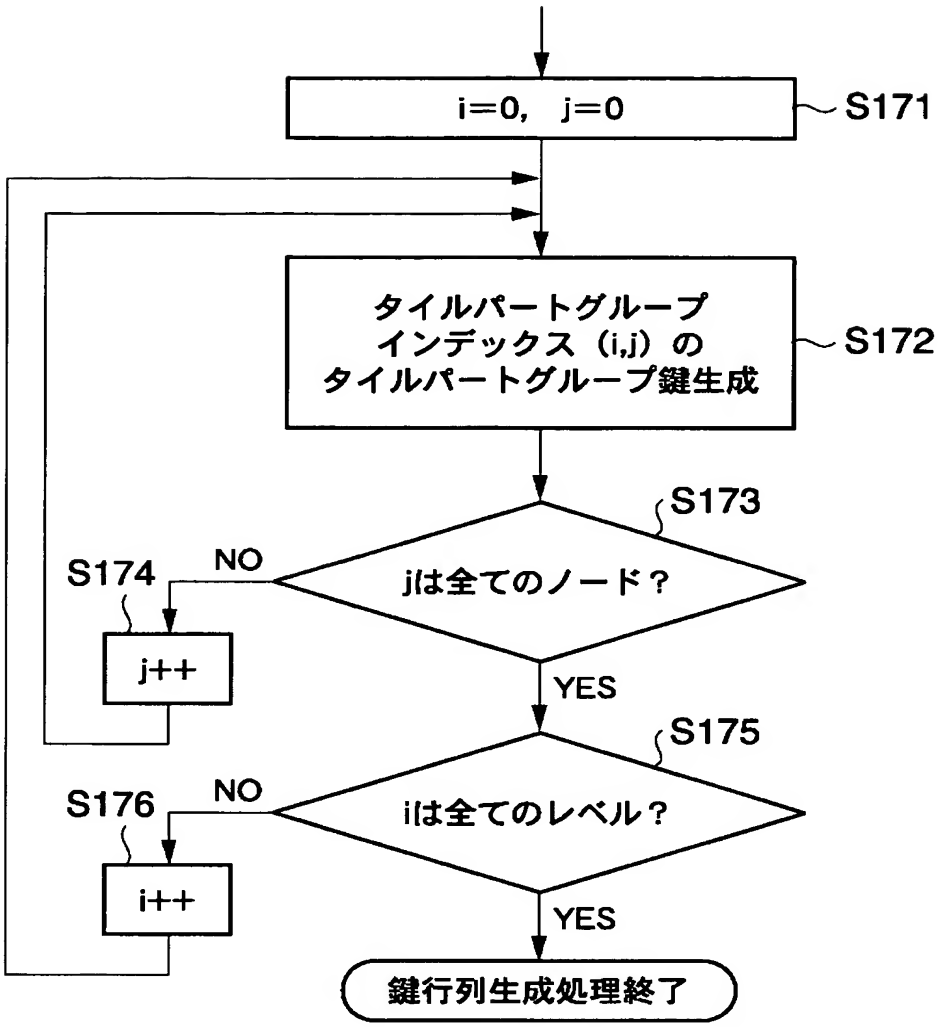
【図１５】



【図１６】



【図１７】


i=0,　j=0
S171
タイルパートグループ
インデックス（i,j）の
タイルパートグループ鍵生成
S172
S173
jは全てのノード？
NO
S174
j++
YES
S175
iは全てのレベル？
NO
S176
i++
YES
鍵行列生成処理終了

【書類名】　要約書

【要約】

【課題】　複数のタイル及び階層構造を有する画像データに対して、タイル及び階層構造毎に異なる暗号鍵を用いて暗号化した場合にも、複数の鍵を管理する必要がないようにする。

【解決手段】　タイル単位に圧縮符号化されたコードストリームｃが入力される。暗号化タイルパート指定部は、隣接する複数のタイルで１つのタイルグループを構成し、更に、隣接するタイルグループで１つの更なるタイルグループを構成することを繰り返すことで、タイルグループの階層構造を定義したとき、どの階層のどのタイルグループについて暗号化を行うかを決定し、暗号化タイル情報ｔａとして出力する。一方、鍵行列生成部１２は、入力したコードストリームｃの全体に対する暗号化鍵ｃｋを生成し、階層構造の各ノードの暗号化鍵を次々に生成し、その結果を鍵行列ｋａとして出力する。暗号化部１３は、暗号化対象となるタイルについては、そのタイル用に生成された鍵を用いて暗号化し、暗号化後野コードストリームｃ’を出力する。

【選択図】　図１

特願２００２－３０４４９８

出　願　人　履　歴　情　報

識別番号　　［０００００１００７］

１．変更年月日　　１９９０年　８月３０日
［変更理由］　　新規登録
住　所　　東京都大田区下丸子３丁目３０番２号
氏　名　　キヤノン株式会社